目次

第 4 章　インストールと設定

第 5 章　運用例

第 6 章　ネットワーク運用

第 7 章　困ったときには

第 8 章　付録

はじめに

このたびは弊社製品をご購入いただき、誠にありがとうございます。
このマニュアルは、セキュリティチップ、指紋センサー、静脈センサー、FeliCa 対応リーダ／ライタ、スマートカードリーダ／ライタ、およびスマートカードホルダー（以降、認証デバイス）の基本的な取り扱い、認証デバイスをお使いになるためのソフトウェアのインストール、および設定と使い方について説明しています。
お使いになる前に、このマニュアル、およびコンピュータ本体のマニュアルをよくお読みになり、正しくお使いいただきますようお願いいたします。

2006 年 10 月

■ セキュリティ機能について

- セキュリティ機能は完全な認証照合、データやハードウェアの保護を保証するものではありません。弊社は、お客様がセキュリティ機能を使用されたこと、または使用できなかったことによって生じるいかなる損害に関しても、一切の責任を負いかねますのであらかじめご了承ください。
- 認証デバイスは、コンピュータ用機器として設計されております。人命に関わる用途、または高度な信頼性、安全性を要する用途での使用は考慮されておりません。このような用途で使用される設備、機器、システム等への組み込みは避けてください。
- 認証デバイスは日本国内仕様であり、添付のアプリケーション、ドライバなどは Windows の日本語版のみ対応しております。

SMARTACCESS のマニュアルについて

認証デバイスをお使いになるためのソフトウェア「SMARTACCESS」には、次のマニュアルを用意しております。目的に合わせてお読みください。

■ SMARTACCESS ファーストステップガイド（認証デバイスをお使いになる方へ）

このマニュアルです。
認証デバイスのドライバインストール手順、設定手順と取り扱い方、および SMARTACCESS のインストール、アンインストールと初期設定手順を説明しています。

■ SMARTACCESS/Premium リファレンスガイド SMARTACCESS/Basic リファレンスガイド

SMARTACCESS の機能全般を説明しています。
このマニュアル内では、まとめて『リファレンスガイド』と表記します。

■ SMARTACCESS/Premium カスタマイズガイド（SMARTACCESS/Premium のみ）

SMARTACCESS をインストールした時点で標準以外の設定で運用するために必要な準備、およびインストール方法について説明しています。

『SMARTACCESS/Premium リファレンスガイド』、および『SMARTACCESS/Premium カスタマイズガイド』は、「SMARTACCESS/Premium」CD-ROM に格納されています。
『SMARTACCESS/Basic リファレンスガイド』は、コンピュータ本体に添付の「ドライバーズディスク」に格納されています。

このマニュアルの表記

■ 本文中の記号

本文中に記載されている記号には、次のような意味があります。

記号	意味
重要	お使いになる際の注意点や、してはいけないことを記述しています。必ずお読みください。
POINT	操作に関連することを記述しています。必要に応じてお読みください。
→	参照ページや参照マニュアルを示しています。

■ キーの表記と操作方法

本文中のキーの表記は、キーボードに書かれているすべての文字を記述するのではなく、説明に必要な文字を次のように記述しています。

例：【Ctrl】キー、【Enter】キー、【→】キーなど

また、複数のキーを同時に押す場合には、次のように「＋」でつないで表記しています。

例：【Ctrl】＋【F3】キー、【Shift】＋【↑】キーなど

■ コマンド入力（キー入力）

本文中では、コマンド入力を次のように表記しています。

```
diskcopy a: a:
        ↑  ↑
```

- ↑の箇所のように文字間隔を空けて表記している部分は、【Space】キーを 1 回押してください。
  また、上記のようなコマンド入力を英小文字で表記していますが、英大文字で入力してもかまいません。
- CD/DVD ドライブなどのドライブ名を、［CD/DVD ドライブ］で表記しています。入力の際は、お使いの環境に合わせて、ドライブ名を入力してください。
  例：［CD/DVD ドライブ］:¥setup.exe

■連続する操作の表記

本文中の操作手順において、連続する操作手順を、「→」でつなげて記述しています。

例：「スタート」ボタンをクリックし、「プログラム」をポイントし、「アクセサリ」をクリックする操作

↓

「スタート」ボタン→「プログラム」→「アクセサリ」の順にクリックします。

また、本文中の操作手順において、操作手順の類似しているものは、あわせて記述しています。

例：「スタート」ボタン→「(すべての) プログラム」→「アクセサリ」の順にクリックします。

■画面例およびイラストについて

表記されている画面およびイラストは一例です。お使いの機種や OS、Web ブラウザなどの環境、またインストールされている認証デバイスによって、画面およびイラストが若干異なることがあります。

■製品の呼び方

本文中の製品名称を、次のように略して表記します。

<table>
<tr><th>製品名称</th><th colspan="3">本文中の表記</th></tr>
<tr><td>認証デバイスを搭載した FMV シリーズ</td><td>パソコン本体</td><td rowspan="2" colspan="2">コンピュータ</td></tr>
<tr><td>認証デバイスを搭載した CELSIUS シリーズ</td><td>ワークステーション本体</td></tr>
<tr><td>セキュリティチップ</td><td>セキュリティチップ</td><td rowspan="6" colspan="2">認証デバイス</td></tr>
<tr><td>FMV シリーズ内蔵スライド方式指紋センサー
指紋認識装置</td><td>指紋センサー</td></tr>
<tr><td>静脈認識装置</td><td>静脈センサー</td></tr>
<tr><td>FeliCa 対応リーダ／ライタ</td><td rowspan="3">リーダ／ライタ</td></tr>
<tr><td>スマートカードリーダ／ライタ</td></tr>
<tr><td>スマートカードホルダー</td></tr>
<tr><td>SMARTACCESS に対応した FeliCa 対非接触 IC カード（FeliCa 対応非接触 IC カード（SMARTACCESS 専用）を含む）</td><td>IC カード（FeliCa 方式）</td><td rowspan="2" colspan="2">カード</td></tr>
<tr><td>スマートカード</td><td>スマートカード</td></tr>
<tr><td>SMARTACCESS/Premium</td><td rowspan="2" colspan="3">SMARTACCESS</td></tr>
<tr><td>SMARTACCESS/Basic</td></tr>
<tr><td>Microsoft® Windows® XP Professional</td><td>Windows XP Professional</td><td rowspan="3">Windows XP</td><td rowspan="6">Windows</td></tr>
<tr><td>Microsoft® Windows® XP Home Edition</td><td>Windows XP Home Edition</td></tr>
<tr><td>Microsoft® Windows® XP Tablet PC Edition 2005</td><td>Windows XP Tablet PC Edition 2005</td></tr>
<tr><td>Microsoft® Windows® 2000 Professional</td><td colspan="2">Windows 2000</td></tr>
<tr><td>Microsoft® Windows Server ™ 2003, Enterprise Edition</td><td>Windows Server 2003</td><td rowspan="2">Windows Server</td></tr>
<tr><td>Microsoft® Windows® 2000 Server</td><td>Windows 2000 Server</td></tr>
</table>

製品名称	本文中の表記
Microsoft® Internet Explorer	Internet Explorer
Microsoft® Outlook® Express	Outlook Express
Microsoft® Office Outlook® 2003	Outlook
Microsoft® Office Word 2003	Word
Netscape® または Netscape® Communicator	Netscape
FENCE-G® V4 以降	FENCE-G

商標および著作権について

Microsoft、Windows は、米国 Microsoft Corporation の、米国およびその他の国における登録商標または商標です。
FeliCa は、ソニー株式会社の登録商標です。
FeliCa は、ソニー株式会社が開発した非接触 IC カードの技術方式です。
PaSoRi（パソリ）は、ソニー株式会社の登録商標です。
その他の各製品名は、各社の商標、または登録商標です。
その他の各製品は、各社の著作物です。

画面の使用に際して米国 Microsoft Corporation の許諾を得ています。

Memo

1

第 1 章

お使いになる前に

認証デバイスや SMARTACCESS をお使いになる前に確認していただくことを説明しています。

1 動作環境

認証デバイスや SMARTACCESS をお使いになる前に、次の条件を確認してください。

重要

- コンピュータに搭載されている認証デバイスをお使いになれます。カスタムメイドで選択していない場合など、機種によってはお使いになれない認証デバイスもあります。

■ 対応機種／ OS

認証デバイスが搭載されている FMV シリーズ、CELSIUS シリーズ／ Windows XP、Windows 2000

注：ハードディスク容量に 50MB 以上の空きがあること

POINT

- セキュア E-mail をお使いになるには、Outlook 2000 以降、Outlook Express 6.0 以降が必要です。
- Word マクロへの署名を利用するには、Word 2000 以降が必要です。
- VeriSign 証明書を利用するには、Internet Explorer 6.0 または Netscape 4.78 ／ 7.0 が必要です。
- アプリケーションログオンは、Internet Explorer 7.0 には対応していません。

■ SMARTACCESS がサポートする認証デバイス

□ SMARTACCESS/Premium

認証デバイス	製品名
セキュリティチップ	FMV シリーズ、および CELSIUS シリーズ内蔵のセキュリティチップ
指紋センサー	FMV シリーズ内蔵スライド方式指紋センサー 指紋認識装置
静脈センサー	PalmSecure™ センサー
FeliCa リーダ／ライタ	FMV-LIFEBOOK 内蔵の FeliCa リーダ／ライタ
スマートカードリーダ／ライタ	FMV シリーズ、および CELSIUS シリーズ内蔵の スマートカードリーダ／ライタ スマートカードホルダー

□ SMARTACCESS/Basic

認証デバイス	製品名
セキュリティチップ	FMV シリーズ､および CELSIUS シリーズ内蔵のセキュリティチップ
指紋センサー	FMV シリーズ内蔵スライド方式指紋センサー
スマートカードリーダ／ライタ	FMV シリーズ、および CELSIUS シリーズ内蔵の スマートカードリーダ／ライタ スマートカードホルダー

Memo

2

第 2 章

認証デバイスについて

認証デバイスをお使いになるための注意事項や基本的な取り扱い方について説明しています。

1 セキュリティチップ

セキュリティチップは、TCG 注1 の仕様に基づいた TPM 注2 と呼ばれる IC チップで TCG セキュリティの基本機能を提供します。セキュリティチップを搭載したコンピュータは、ソフトウェアによる攻撃および物理的な攻撃からデータを保護し、より強固なセキュリティを実現します。
セキュリティチップは内部に暗号鍵を保持し、Windows ログオンやアプリケーションログオンで使用するパスワードなどを暗号化できます。セキュリティチップで管理された暗号鍵は外部に出す方法がないので、万一データが外部に持ち出されたとしても、データの内容を復号化することはできません。また、ユーザーごとに鍵を生成することができるので、データを安全に管理することができます。

注 1：TCG は Trusted Computing Group の略称です。
TCG は、信頼性と安全性を持った新しいコンピュータをつくるためのオープンな業界仕様を策定する団体です。
（https://www.trustedcomputinggroup.org/）
注 2：TPM は Trusted Platform Module の略称です。

セキュリティ機能の概要

セキュリティチップは、各利用者に固有の鍵を生成し、証明書を管理します。この鍵と証明書を用いることにより、セキュリティチップは暗号化や認証を行います。セキュリティチップ内に保有する鍵は、取り出すことが不可能なため鍵の解読ができません。そのため暗号化されたデータや認証は安全に行われます。利用者はこの鍵と証明書を利用するためのパスワードを設定します。

セキュリティチップを利用するために、SMARTACCESSの他、Security Platform（Infineon TPM Professional Package）を使用します。
これにより、次のことが行えるようになります。

■ IEEE802.1x 認証ファイルの管理

IEEE802.1x にて利用する証明書をセキュリティチップで管理することができます。

■ ファイルとフォルダの暗号化－ Windows 暗号化ファイルシステム（EFS）

ユーティリティでファイルとフォルダの暗号化を設定することにより、EFS による暗号化に利用される鍵をセキュリティチップで安全に保管します。
詳しくは「運用例」－「セキュリティチップで暗号化ファイルの鍵を保護する」（→ P.112）をご覧ください。

■ セキュア E-Mail

ユーティリティで E-Mail の保護を設定することにより、E-Mail の暗号用の証明書をセキュリティチップで安全に管理します。

■Word マクロへの署名

ユーティリティでセキュリティ機能を設定することにより、Word マクロへの署名をセキュリティチップで安全に保護します。

■ログオン認証

セキュリティチップで暗号化された ID やパスワードを使って、Windows やソフトウェアなどへのログオン認証ができます。また、ユーザー情報をセキュリティチップで暗号化して、安全に保存することができます。
セキュリティチップを使ってWindowsやソフトウェアにログオンするときは、セキュリティチップに対するパスワード（ユーザーキーパスワード）を使用します。
ユーザーキーパスワードは、通常の Windows パスワードよりも長い文字列を扱うことができるため、セキュリティを高めることができます。
ユーザーキーパスワードを入力すると、セキュリティチップによって暗号化されたユーザー名やパスワードを復号化できます。ユーザーキーパスワードを 1 つだけ覚えれば、複雑なパスワードをアプリケーションごとに覚える必要はありません。
詳しくは、『リファレンスガイド』の「機能編」－「Windows ログオン」、「アプリケーションログオン」をご覧ください。

■コンピュータの不正なハードウェアの変更の検出

SMARTACCESS の「機器監査」機能をお使いになると、Windows ログオン時にコンピュータの機器構成のチェックを行います。ハードウェア構成または設定が不正に変更されていることを検出した場合に、警告を表示したり、Windows ログオンを拒否したりすることができます。
これにより、ユーザーが離席中など気付かないうちにハードウェアを変更されても、検出することができます。
機器監査の設定については、『リファレンスガイド』の「機能編」－「Windows ログオン」－「機器監査」をご覧ください。
なお、不正にコンピュータの設定が変更されたときだけでなく、修理により設定が変更された場合でも機器監査変更が検出されることがあります。修理に出す前に「コンピュータの修理や保守を依頼する場合」（→ P.19）をご覧になり、設定を変更できるようにしてください。
ハードウェアの変更については次の項目が検出されます。

- BIOS のハードウェア構成
- メモリスロットの構成
- USB ポートに、USB メモリなどのストレージデバイスを接続したとき
- ハードディスクドライブ構成（FMV-W シリーズの場合）
- PCI スロットの構成、およびグラフィックボード（FMV-ESPRIMO シリーズ、FMV ロングライフパソコン、および CELSIUS シリーズの場合）
- モバイルマルチベイ、およびマルチベイ（FMV-LIFEBOOK シリーズの場合）

重要

- FMV-W シリーズの場合、ハードウェアや BIOS 設定の変更を元に戻しても、機器監査の状態が元に戻らないことがあります。そのため、誤って変更してしまったり、変更後に機器監査の再登録を行わなかったりすると、Windows にログオンできなくなります。
  その場合は、機器構成を登録し直す必要があります。

POINT

- ハードウェアの変更については、休止状態からの復帰時にも確認されます。

セキュリティチップの管理

セキュリティチップには、セキュリティチップの管理を行う「所有者」とセキュリティチップを使用する「ユーザ」を登録します。
「所有者」および「ユーザ」は次の鍵および証明書やファイルを作成・利用します。

POINT

- SMARTACCESS の「管理者」、「利用者」と Security Platform（Infineon TPM Professional Package）の関係は、次のようにしてお使いになることをお勧めします。

SMARTACCESS	Security Platform（Infineon TPM Professional Package）
管理者	所有者
利用者	ユーザ

■「所有者」が管理するもの

□ 所有者キーと所有者パスワード

所有者は、所有者であることを証明するキーを作成します。この鍵はセキュリティチップにより保護され、所有者パスワードを入力することによって利用することができます。
所有者パスワードは忘れないよう注意してください。

□ 自動バックアップファイルと復元用トークン

セキュリティチップで管理しているすべての鍵や証明書のバックアップを行います。
バックアップはスケジュールを設定することにより定期的に行うことができます。
セキュリティチップが故障しても、新しいコンピュータでこのファイルを用いて復元することにより、以前利用していた暗号化ファイルなどが利用できるようになります。
自動バックアップファイルは、トークンにより暗号化されています。自動バックアップファイルを利用する場合には、トークンファイルとそのパスワードが必要です。トークンファイルを失くしたり、パスワードを忘れたりしないよう注意して管理してください。

□ パスワードリセットファイルとリセットトークン

「ユーザ」がセキュリティチップのパスワードを忘れた場合に備えて、前もってパスワードリセット用のファイルを作成しておくことで現状のパスワードを新規パスワードに変更することができます。所有者はあらかじめパスワードリセットの設定を行い、必要に応じて「ユーザ」のパスワードを設定し直します。
パスワードリセットファイルは、トークンにより暗号化されています。パスワードリセットファイルを利用する場合には、トークンファイルとそのパスワードが必要です。トークンファイルを失くしたり、パスワードを忘れたりしないよう注意して管理してください。

■「ユーザ」が管理するもの

□ ユーザーキーとユーザーキーパスワード

「ユーザ」はセキュリティチップを利用する場合、ユーザーキーを作成します。このキーはセキュリティチップにより保護され、ユーザーキーパスワードを入力することによって利用することができます。キーを紛失した場合は、それ以前に暗号化していたデータやファイルなどを再び利用することができなくなります。管理には注意してください。また、パスワードを忘れた場合も、キーが利用できなくなるため、それまでに暗号化していたデータやファイルを再び利用することができなくなります。パスワードは忘れないよう注意してください。

鍵や証明書、パスワードの管理について

セキュリティチップは、複数の鍵や証明書を扱います。これらの鍵や証明書を紛失した場合は、その鍵によって暗号化されたファイルなどは利用できなくなることがありますので注意してください。またこれらの鍵を利用する場合はパスワードが必要です。パスワードを正しく入力しないと鍵が利用できないため、紛失時と同様に暗号化されたファイルなどが利用できなくなります。

■ パスワードの変更

セキュリティチップに設定した、所有者パスワードおよびユーザーキーパスワードは変更することができます。また、ユーザーキーパスワードは各ユーザで定期的に変更することをお勧めします。

- 「所有者パスワード」の変更については、『リファレンスガイド』の「ツール編」－「環境設定」－「ユーザー情報管理」－「セキュリティチップ」をご覧ください。
- 「ユーザーキーパスワード」の変更については、『リファレンスガイド』の「ツール編」－「ユーザー情報設定」－「ユーザー情報管理」－「セキュリティチップ」、および「環境設定」－「ユーザー情報管理」－「セキュリティチップ」をご覧ください。

■ パスワードを忘れた場合には

ユーザーキーパスワードを忘れた場合は、再設定することができます。
ユーザーキーパスワードを再設定する場合には、所有者が事前にパスワードリセットの設定を行う必要があります。
パスワードをリセットする場合は、、『リファレンスガイド』の「ツール編」－「環境設定」－「ユーザー情報管理」－「セキュリティチップ」をご覧ください。

■ 新しいユーザーを登録するには

Windows に新規ユーザーを追加する場合、そのユーザーがセキュリティチップを利用するためには、セキュリティチップに新規ユーザーの情報を登録する必要があります。SMARTACCESS では Windows へ新規ユーザーを追加し、セキュリティチップの登録を行うことができます。

運用上の注意

セキュリティチップを利用するための環境設定が完了すると、ファイルやフォルダの暗号化、メールの証明書の管理などがより安全な環境で運用することができるようになります。
次の場合は、注意事項に従って運用してください。

・通常備えておくこと（→ P.18）
・ハードウェアの変更を行う場合（→ P.19）
・コンピュータの修理や保守を依頼する場合（→ P.19）
・コンピュータをリカバリする場合、または SMARTACCESS を再インストールする場合（→ P.20）
・コンピュータを廃棄する場合（→ P.21）

■通常備えておくこと

次のような場合、セキュリティチップが利用できなくなることがあります。

・セキュリティチップの故障時
・ハードディスクのリカバリ後
・コンピュータの部品の交換後

このような場合に備えて、必ずセキュリティチップの鍵を定期的にバックアップするよう設定を行ってください。
バックアップファイルを紛失したり、パスワードを忘れたりすると、セキュリティチップが利用できなくなります。バックアップファイルやその時に設定したパスワードは、紛失したり忘れたりしないよう注意して管理してください。

□ バックアップ

「所有者」でログオンした時に、画面右下の通知領域からバックアップについて表示されるメッセージに従い、バックアップを行ってください。
「所有者」はセキュリティチップのバックアップと各「ユーザ」のバックアップを行う必要があります。
各「ユーザ」でバックアップを行う必要はありませんが、復元を行った後、ユーザーキーパスワードを入力する必要があります。
バックアップの手順については、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧ください。

重要

▶ 手順に従わずにファイルや設定の変更を行うと、セキュリティチップで管理していた環境が利用できなくなることがあります。

□ リストア

リストアは、セキュリティチップで保護された環境に変更があった場合、以前の環境を引き続き利用するための作業です。
「所有者」がセキュリティチップのリストアを行います。
「ユーザ」は、リストアを行う必要はありませんが、「所有者」がリストアを行った後にユーザーキーパスワードを入力する必要があります。
リストアの手順については、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧ください。

重要

- リストアは、セキュリティチップの所有者パスワードによって保護されています。そのため、リストアはセキュリティチップの「所有者」が行う必要があります。
- 手順に従わずにファイルや設定の変更を行うと、セキュリティチップで管理していた環境が利用できなくなることがあります。

■ハードウェアの変更を行う場合

「機器監査」機能（→ P.15）をお使いの場合、ハードウェアの設定を変更すると、Windows にログオンできなくなることがあります。ハードウェアの変更を行う前には必ず、「SMARTACCESS による Windows ログオン」を使用しない設定に変更してください。「パスワードの自動生成」を行っている場合は、一度「パスワードの自動生成」の設定を解除した後、「パスワードの変更」より任意のパスワードに変更してから「SMARTACCESS による Windows ログオン」機能の解除を行ってください。
また、ハードウェアの変更後に、再度「現在の機器構成情報の登録」を行う必要があります。
詳しくは『リファレンスガイド』の「機能編」－「Windows ログオン」をご覧ください。

■コンピュータの修理や保守を依頼する場合

□ 修理前に必要な作業

鍵のバックアップ

「バックアップ」（→ P.18）をご覧になり、バックアップを行います。

「SMARTACCESS による Windows ログオン」を使用しない設定に変更する

必ず「SMARTACCESS による Windows ログオン」の設定を解除してください。
「SMARTACCESS による Windows ログオン」の設定を解除していないと、修理や保守ができないことがあります。また、「SMARTACCESS による Windows ログオン」の設定を解除せずに、修理すると、Windows にログオンできなくなることがあります。
解除の手順は次のとおりです。

1. **SMARTACCESS をインストールしたときと同じアカウントで Windows にログオンします。**

2. **「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。**
   「環境設定」が表示されます。

3. **「設定項目一覧」から「ログオン認証」→「Windows ログオン」の順にクリックします。**

4. **パスワードの自動生成を行っている場合は、パスワードの自動生成を「しない」に設定します。**
   パスワードの自動生成を行っていない場合は、手順 6 に進んでください。

5. **次の手順で Windows パスワードを任意のパスワードに変更します。**
   1. 「スタート」ボタン→「コントロールパネル」の順にクリックします。
      「コントロールパネル」ウィンドウが表示されます。

2.「ユーザー アカウント」をクリックします。
「ユーザー アカウント」ウィンドウが表示されます。
3. パスワードを変更するアカウントをクリックします。
4.「パスワードを変更する」をクリックします。

この後はメッセージに従って操作します。

6 **「SMARTACCESS による Windows ログオン」の「使用しない」にチェックし、「OK」をクリックします。**

詳しくは、『リファレンスガイド』の「機能編」－「Windows ログオン」をご覧ください。

BIOS パスワードを解除する

コンピュータ本体の『製品ガイド』の「BIOS」－「BIOS のパスワード機能を使う」をご覧になり、設定した管理者用パスワードを解除してください。

□ 修理後に必要な作業

リストアする

「リストア」（→ P.18）をご覧になり、鍵を復元してください。

重要

- **リストアは、パスワードの入力などが必要なため、弊社で行うことはできません。『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧になり、注意して復元してください。**

BIOS パスワードを設定する

コンピュータ本体の『製品ガイド』の「BIOS」－「BIOS のパスワード機能を使う」をご覧になり、パスワードを設定してください。

「SMARTACCESS による Windows ログオン」を使用する設定に変更する

「SMARTACCESS による Windows ログオン」を使用していた場合は、『リファレンスガイド』の「機能編」－「Windows ログオン」をご覧になり、「SMARTACCESS による Windows ログオン」の設定を「する」に変更してください。
なお、「SMARTACCESS による Windows ログオン」の設定を変更する前に、「現在の機器構成情報の登録」を行う必要があります。

■ コンピュータをリカバリする場合、または SMARTACCESS を再インストールする場合

認証デバイスとしてセキュリティチップがインストールされている環境でリカバリをする場合、または SMARTACCESS を再インストールする場合は、あらかじめ BIOS セットアップでセキュリティチップの鍵を消去する必要があります。
セキュリティチップの鍵の消去については、コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧ください。
なおセキュリティチップの鍵を消去すると、それまで使用していた鍵や証明書が使用できなくなります。セキュリティチップで管理されている鍵や証明書の情報を引き続きお使いになるには、SMARTACCESS をアンインストールする前にバックアップし、再インストール後にリストアを行なう必要があります。
バックアップとリストアの手順については、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧ください。

■コンピュータを廃棄する場合

コンピュータを廃棄する場合、パソコンに残ったデータを復元できないようにすることが重要です。セキュリティチップにより保護されたデータは、セキュリティチップの鍵を消去し、復元用ファイルを破棄することで復元することができなくなります。
次の手順に従って、鍵の消去とハードディスク内のデータ削除を行ってください。

重要

- セキュリティチップの鍵や、鍵に関連するファイルを削除すると、セキュリティチップで暗号化したファイルや証明書が利用できなくなります。
  削除する前に、必要に応じて暗号化を解除してください。
- セキュリティチップの鍵を消去しても、ハードディスク内のデータは破棄されません。
  セキュリティチップで保護されたハードディスク内のデータは見ることができなくなりますが、必ずハードディスクのデータも削除してください。

1 **セキュリティチップの鍵を消去します。**
消去の手順については、コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧ください。

2 **コンピュータ本体の『製品ガイド』の「セキュリティ」－「パソコン本体廃棄時のセキュリティ」をご覧になり、ハードディスク内のデータを削除します。**

2 指紋センサー

人により異なる特徴を持つ「指紋」を利用した認証ができます。また、指をスライドさせるだけの簡単な操作で本人認証ができ、他人にパスワードを盗み見られる心配がありません。

セキュリティ機能の概要

■ログオン認証

ログオン用の ID やパスワードをコンピュータに登録した指紋情報と関連付けることにより、指紋の読み取りで Windows やソフトウェアなどにログオンすることができます。
いったんユーザー情報と指紋情報を関連付けてしまえば、複雑なパスワードをソフトウェアごとに覚える必要がなく、パスワードを盗み見られる心配もありません。
詳しくは、『リファレンスガイド』の「機能編」－「Windows ログオン」、「アプリケーションログオン」をご覧ください。

■BIOS 指紋認証

コンピュータの不正使用を防止するための BIOS のパスワード機能を、指紋情報と組み合わせて使用することができます。コンピュータの起動時やスタンバイからレジュームするときに、キーボードから BIOS パスワードを入力する代わりに、指紋の読み取りで認証する機能です。
この機能は、BIOS 指紋認証機能に対応しているコンピュータで使用可能です。
詳しくは、「運用例」－「BIOS 指紋認証による Windows ログオン」(→ P.122)をご覧ください。

運用上のご注意

■通常備えておくこと

コンピュータの修理や保守を行うと、SMARTACCESS の設定がリセットされることがあります。そのような場合に備えて、必ず SMARTACCESS の設定を定期的にバックアップするよう設定を行ってください。
バックアップファイルは、紛失しないよう注意して管理してください。
バックアップの手順については、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧ください。

■コンピュータの修理や保守を依頼する場合

□ 修理前に必要な作業

SMARTACCESS の設定のバックアップ

『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧になり、バックアップを行います。

「SMARTACCESS による Windows ログオン」を使用しない設定に変更する

必ず「SMARTACCESS による Windows ログオン」の設定を解除してください。
「SMARTACCESS による Windows ログオン」の設定を解除していないと、修理や保守ができないことがあります。また、「SMARTACCESS による Windows ログオン」の設定を解除せずに、修理すると、Windows にログオンできなくなることがあります。
解除の手順は次のとおりです。

1 **SMARTACCESS をインストールしたときと同じアカウントで Windows にログオンします。**

2 **「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。**

「環境設定」が表示されます。

3 **「設定項目一覧」から「ログオン認証」→「Windows ログオン」の順にクリックします。**

4 **パスワードの自動生成を行っている場合は、パスワードの自動生成を「しない」に設定します。**

パスワードの自動生成を行っていない場合は、手順 6 に進んでください。

5 **次の手順で Windows パスワードを任意のパスワードに変更します。**

1. 「スタート」ボタン→「コントロールパネル」の順にクリックします。
   「コントロールパネル」ウィンドウが表示されます。
2. 「ユーザー アカウント」をクリックします。
   「ユーザー アカウント」ウィンドウが表示されます。
3. パスワードを変更するアカウントをクリックします。
4. 「パスワードを変更する」をクリックします。

この後はメッセージに従って操作します。

6 **「SMARTACCESS による Windows ログオン」の「使用しない」にチェックし、「OK」をクリックします。**

詳しくは、『リファレンスガイド』の「機能編」－「Windows ログオン」をご覧ください。

□ 修理後に必要な作業

リストアする

『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧になり、リストアを行います。

「SMARTACCESS による Windows ログオン」を使用する設定に変更する

「SMARTACCESS による Windows ログオン」を使用していた場合は、『リファレンスガイド』の「機能編」－「Windows ログオン」をご覧になり、「SMARTACCESS による Windows ログオン」の設定を「する」に変更してください。

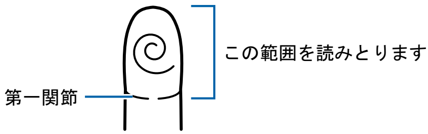
取り扱い方

■指紋を読み取る

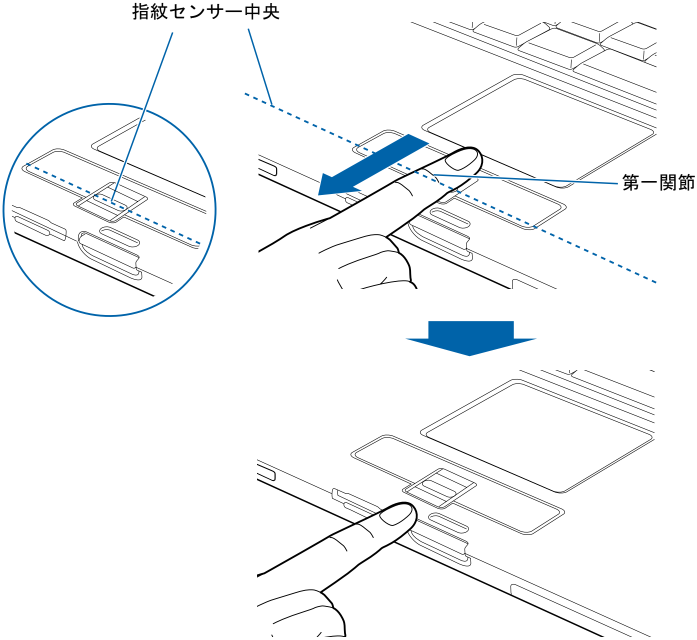
指紋の登録や認証を行う場合は、次のように指をスライドさせてください。認証の失敗を減らすことができます。

1 操作する指の第一関節が、指紋センサーの中央部に当たるように準備します。

第一関節より先の部分が読み取り範囲となります。



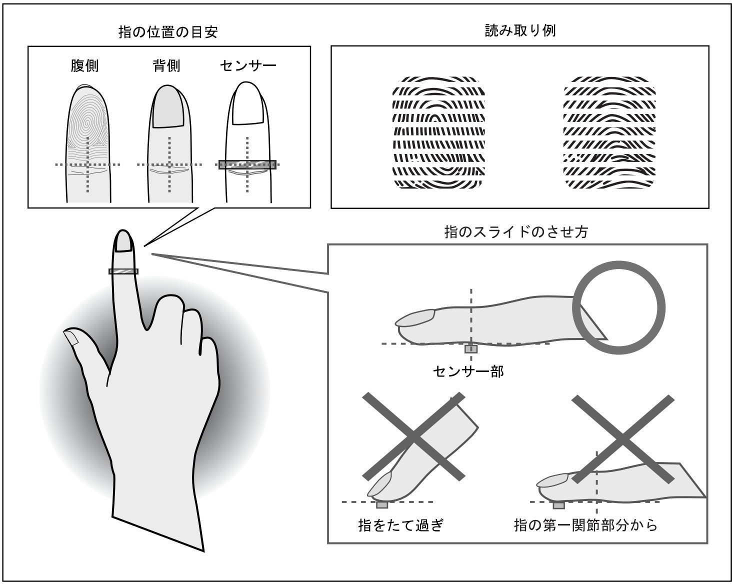
2 第一関節を指紋センサーに押し当てると同時に指を動かし、センサー部が完全に見えるまで水平にスライドします。



（イラストは機種や状況により異なります）

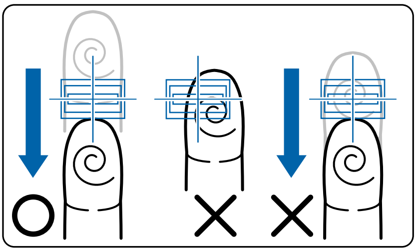
□ 指のスライドのさせ方について

正しく指紋を読み取らせるため、次の図のように指を置いてください。



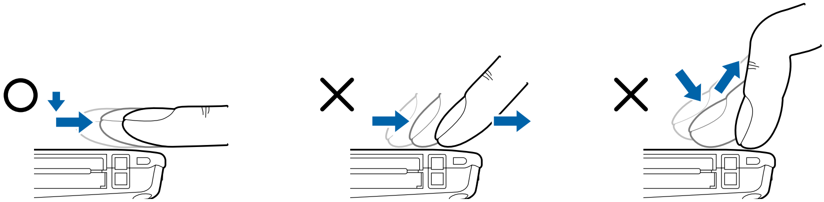
重要

- うまく認識されないときは
  次の点に気を付けて操作してください。
  ・指の第一関節より先の部分が、指紋センサー上を通過するようにする
  ・指紋の渦の中心が、指紋センサーの中心を通過するようにする
  ・1 秒程度で通過するくらいの速さで、スーッと動かす



なお、親指など、指紋の渦の中心を合わせにくい指は、うまく認識できないことがあります。その際は、中心を通過させやすい指を登録してください。

- 指を突き立てたり、引っかけるようにスライドさせないでください。
  指紋センサーに指のはら（指紋の中心部）が接触していなかったり、指を引っかけるようにスライドさせると指紋の読み取りがうまくいかない場合があります。
  必ず、指のはら（指紋の中心部）が指紋センサーに接触するようにスライドさせてください。



（イラストは機種や状況により異なります）

- 指紋の読み取りがうまくいかない場合
  - 指のスライドが速すぎたり遅すぎたりした場合、正常に認識できないことがあります。画面のメッセージに従って、スライドの速さを調節してください。
  - 外付けの指紋センサーをお使いの場合、指紋センサーを置いた台などの表面の状態によっては、指をスライドさせたときに指紋センサーが滑ることがあります。底面のラバーが密着しやすい場所で操作するか、他方の手で押さえながら操作してください。

■ 指紋センサーのスクロール機能を使用する（FMV-LIFEBOOK 内蔵スライド方式指紋センサーの場合）

指紋センサードライバをインストールすると、指紋センサーのスクロール機能で、画面のスクロールができるようになります。ウィンドウ内のスクロールする領域をクリックしてから、指紋センサー上で指先を前後方向にスライドすると、指の動きに合わせてウィンドウ内の表示が上下にスクロールします。

POINT

- 対象とするウィンドウによっては、スクロール機能が使用できない場合があります。
- スクロールの速度については、「コントロールパネル」の「指紋センサー」から調整することができます。「指紋センサー」が表示されていない場合は、ウィンドウ左側の「コントロールパネルのその他のオプション」をクリックしてください。

■ 取り扱い上の注意事項

□ 指紋センサー使用時のご注意

・センサー部に強い衝撃を与えないでください。故障の原因となることがあります。

□ 指紋登録時／照合時のご注意

・指の状態が次のような場合には、指紋の登録が困難になったり、照合率が低下することがあります。
  - 汗や脂が多い
  - 手が荒れたり、極端に乾燥している
  - 指に傷がある、または磨耗して指紋が薄い
  - 急に太ったり、やせたりして指紋が変化した

  手を洗う、手を拭く、登録する指を変えるなどお客様の指の状態に合わせて対処することで、登録時や照合時の状況が改善されることがあります。

・指紋の登録や照合を行う場合、センサー上で指を正しくスライドさせてください（→P.24）。スライドのさせ方が正しくないと、指紋の中心がセンサー中央からずれて、指紋を読み取ることが困難になったり、照合率が低下することがあります。

□ センサーに関するご注意

・指紋の読み取りを行う前に金属に手を触れるなどして、静電気を取り除いてください。静電気が故障の原因となる場合があります。冬季など乾燥する時期は特にご注意ください。
・センサー部分をひっかいたり、先のとがったもので押したりしないでください。傷がつく原因となります。
・使用中はセンサー表面が温かくなることがありますが、故障ではありません。

□ センサー表面の清掃について

・次のような場合は指紋の読み取りが困難になったり、照合率が低下することがあります。センサー表面はときどき清掃してください。
  - センサー表面がほこりや皮脂などで汚れている
  - センサー表面に汗などの水分が付着している
  - センサー表面が結露している
・次のような現象が起きる場合は、センサー表面を清掃してください。現象が改善されることがあります。
  - 指を置いていないのに「初期化中に画像を検出しました」というエラーが表示される
  - 指を離しているのに「指を離してください」の表示が出たままになる
  - 認証画面から「バイオパスワード認証」ウィンドウに切り替えられない
  - 指紋の登録失敗や照合失敗が頻発する
・清掃の際には、乾いたやわらかい布でセンサー表面の汚れを軽く拭き取ってください。

重要

▶ センサー表面に水などの液体をかけないでください。また、ベンジンなどの揮発性有機溶剤や化学ぞうきんは使用しないでください。

3 静脈センサー

「静脈」は、本数が多く線のカーブや分岐などが複雑なため個人情報量が多いことから、認識率が高く個人差も出やすいです。「静脈」を利用した認証では、手のひらの静脈を使って本人かどうか判断します。センサーに手のひらをかざすだけの簡単な操作で認証ができ、盗難や忘却、偽造などの心配がありません。
静脈センサーの詳しい取り扱い方法などは、静脈センサーに添付のマニュアルをご覧ください。

セキュリティ機能の概要

■ログオン認証

ログオン用の ID やパスワードをコンピュータに登録した静脈情報と関連付けることにより、静脈の読み取りで Windows やソフトウェアなどにログオンすることができます。
いったんユーザー情報と静脈情報を関連付けてしまえば、複雑なパスワードをソフトウェアごとに覚える必要がなく、パスワードを盗み見られる心配もありません。
詳しくは、『リファレンスガイド』の「機能編」－「Windows ログオン」、「アプリケーションログオン」をご覧ください。

運用上のご注意

■通常備えておくこと

コンピュータの修理や保守を行うと、SMARTACCESS の設定がリセットされることがあります。そのような場合に備えて、必ず SMARTACCESS の設定を定期的にバックアップするよう設定を行ってください。
バックアップファイルは、紛失しないよう注意して管理してください。
バックアップの手順については、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧ください。

■コンピュータの修理や保守を依頼する場合

□ 修理前に必要な作業

SMARTACCESS の設定のバックアップ

『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧になり、バックアップを行います。

「SMARTACCESS による Windows ログオン」を使用しない設定に変更する

必ず「SMARTACCESS による Windows ログオン」の設定を解除してください。
「SMARTACCESS による Windows ログオン」の設定を解除していないと、修理や保守ができないことがあります。また、「SMARTACCESS による Windows ログオン」の設定を解除せずに、修理すると、Windows にログオンできなくなることがあります。
解除の手順は次のとおりです。

1 **SMARTACCESS をインストールしたときと同じアカウントで Windows にログオンします。**

2 **「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。**
「環境設定」が表示されます。

3 **「設定項目一覧」から「ログオン認証」→「Windows ログオン」の順にクリックします。**

4 **パスワードの自動生成を行っている場合は、パスワードの自動生成を「しない」に設定します。**
パスワードの自動生成を行っていない場合は、手順 6 に進んでください。

5 **次の手順で Windows パスワードを任意のパスワードに変更します。**
1. 「スタート」ボタン→「コントロールパネル」の順にクリックします。
   「コントロールパネル」ウィンドウが表示されます。
2. 「ユーザー アカウント」をクリックします。
   「ユーザー アカウント」ウィンドウが表示されます。
3. パスワードを変更するアカウントをクリックします。
4. 「パスワードを変更する」をクリックします。

この後はメッセージに従って操作します。

6 **「SMARTACCESS による Windows ログオン」の「使用しない」にチェックし、「OK」をクリックします。**

詳しくは、『リファレンスガイド』の「機能編」－「Windows ログオン」をご覧ください。

□ 修理後に必要な作業

リストアする

『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧になり、リストアを行います。

「SMARTACCESS による Windows ログオン」を使用する設定に変更する

「SMARTACCESS による Windows ログオン」を使用していた場合は、『リファレンスガイド』の「機能編」－「Windows ログオン」をご覧になり、「SMARTACCESS による Windows ログオン」の設定を「する」に変更してください。

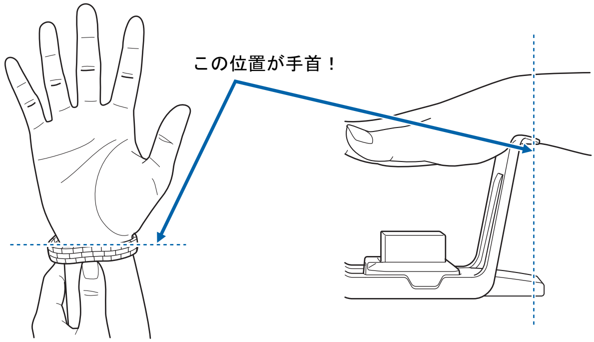
取り扱い方

■手のかざし方

静脈データの登録や認証を行う場合は、次のように静脈センサーに手をかざしてください。

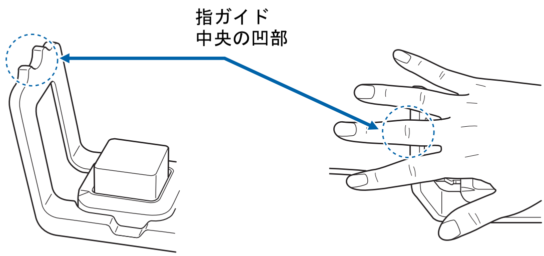
1 手首を手首ガイドに乗せます。

手首とは、腕時計のベルトを手のひら側に寄せたときの、ベルトの位置となります。この位置を、手首ガイドに乗せてください。



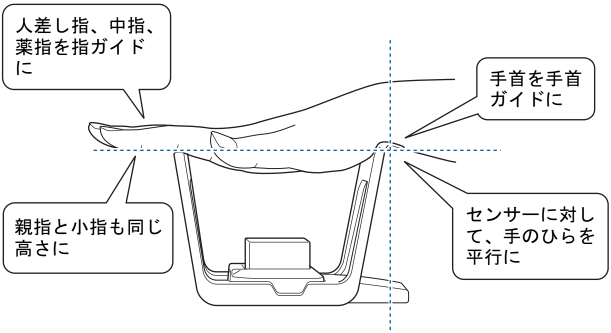
2 人差し指、中指、薬指を指ガイドに乗せます。

指ガイド中央の凹部に、中指を合わせてください。



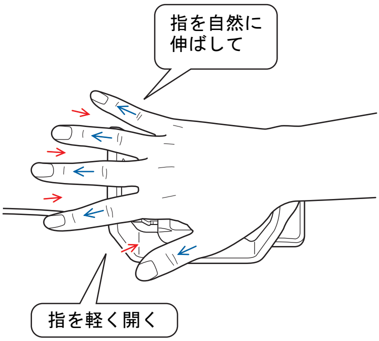
3 親指と小指を、人差し指、中指、薬指と同じ高さに揃えます。

4 センサーに対して、手のひらが平行になっていることを確認します。



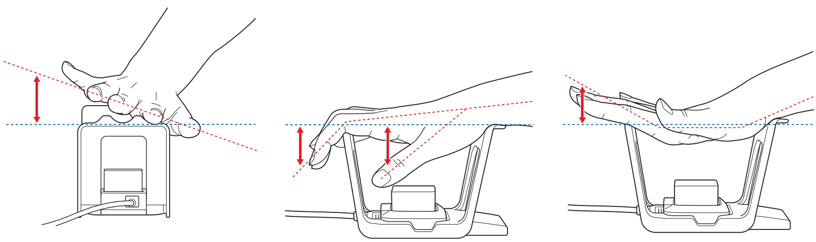
5 指を自然に伸ばします。

6 親指も含め、すべての指を軽く開きます。



重要

- 撮影中は手を動かさないでください。手が動いている状態では、正しく撮影することができません。
- 次のような手のかざし方をすると、正しく撮影することができません。
  - ・センサーに対して、手のひらが平行になっていない。
  - ・指が伸びていない。
  - ・指がそっている。
  - ・指が開かれていない。特に親指が開かれていない。
  - ・手首の位置が正しくない。



POINT

- 手が小さく、指先が指ガイドに届かない場合、手のかざし方が正しくても、指先が垂れてしまうことがあります。このようなときは、指先を指ガイドに乗せ、手首ガイドには腕を乗せてください。手のかざし方が安定します。

■取り扱い上の注意事項

□ 静脈センサーの人体への影響について

静脈センサーは、近赤外光を用いて、非接触で手のひら静脈を撮影する装置です。近赤外光は、ACGIH 注の曝露基準値の 10mW/ cm^2 以下です。人間には視覚できませんが、人体への影響はありません。
また、センサーは、レーザー製品の国際規格である (IEC 60825-1:2001)、CENELEC 規格 (EN 60825-1:1994+A1:2002+A2:2001)、および JIS 規格 (JIS C6802:2005) のクラス 1 に適合しています。

注：American Conference of Governmental Industrial Hygienists

□ 静脈センサーの取り扱いについて

・静脈センサーの接続や取り外しは、コンピュータの電源を切った状態で行ってください。コンピュータの起動中に接続や取り外しを行うと、静脈センサーが正常に動作しなくなる場合があります。
・コンピュータがスタンバイまたは休止状態になると、静脈センサーが正常に動作しなくなる場合があります。

□ 照明環境について

静脈センサーは、近赤外光を用いて、非接触で手のひら静脈を撮影する装置です。
近赤外光を用いた装置の認証精度は、自然光（太陽光）、白熱灯やハロゲン灯などの近赤外光を多く含んだ照明環境に大きく左右されます。
静脈センサーをお使いになる照明環境の目安は次のとおりです。

照明の種類	明るさ
自然光	2000 ルクス以下注
蛍光灯	2000 ルクス以下
白熱灯 ハロゲン灯	500 ルクス以下

注：自然光は、可視光照度計を照射方角に向けて測定してください。
　可視光照度計とは、目に見える明るさを測定する計器で、その場所の明るさを測定する場合に使用します。
　通常、一般の事務所で、500 ～ 1500 ルクスです。

重要

- 直射日光が当たる場所などには設置しない
  次のような場所ではお使いにならないでください。静脈センサーが正常に動作しなくなる恐れがあります。
  ・太陽光が直接当たる場所
  ・太陽光が近辺まで差し込む場所
  ・西日があたる場所
  なお、このような場所でお使いになる場合は、周辺の窓にカーテンやブラインドなどを取り付け、直射日光を遮断してください。

▶ 白熱灯やハロゲン灯を使用する場合
白熱灯やハロゲン灯は、可視光照度計で測定した値よりも、2 ～ 4 倍の照度があります。白熱灯やハロゲン灯をお使いになる場合は、センサー面を直射しないよう、角度を調整してください。それでも静脈センサーが正常に動作しないときは、蛍光灯に交換してください。

▶ 赤外線を発光する機器の近くで使用する場合
静脈センサーは、リモコンなどの赤外線を発光する機器の近くで使用すると、正常に動作しなくなる恐れがあります。赤外線を発光する機器から、50cm 以上離れた場所でご使用ください。

□ 静脈データ登録時のご注意

静脈センサーの認証精度は、登録されている静脈データの品質に大きく左右されます。
登録されている静脈データの品質が低いと、本人認証時に認証できない状態が多発する原因となります。手のひら静脈を撮影して静脈データを登録するときは、正しい手のかざし方で登録してください（→ P.30）。
手のひらの状態が次のような場合、手のひら静脈を正しく撮影できず、登録される静脈データの品質が低くなったり、静脈データを登録することができなかったりすることがあります。

・手のひらに、絆創膏や包帯をつけている
・手袋や、ブレスレットなどをしている
・手のひらが汚れている、または傷などがある
・手のひらが濡れている

□ 本人認証時のご注意

次の場合、正しく認証できない可能性があります。

・静脈データ登録時と認証時で、手のかざし方を変えた。
・手のひらの状態が、静脈データ登録時から変わってしまった。

本人認証するときは、正しい手のかざし方で行ってください（→ P.30）。正しく認証できない状態が多発する場合、静脈データを登録し直すことをお勧めします。

4 FeliCa 対応リーダ／ライタ

FeliCaは、ソニー株式会社が開発した非接触ICカードの技術方式です。コンピュータに内蔵のFeliCa対応リーダ／ライタを利用して、コンピュータのセキュリティを向上するための環境を提供します。

重要

- FeliCa 対応リーダ／ライタをお使いになるには、SMARTACCESS/Premium が必要です。

セキュリティ機能の概要

■ログオン認証

Windows やソフトウェアなどの ID やパスワードを IC カード（FeliCa 方式）に格納して、ログオン認証に使うことができます。
IC カード（FeliCa 方式）を使ってログオンするときは、カードを FeliCa 対応リーダ／ライタにタッチまたは置く（セットする）ことで認証されます。カードにソフトウェアごとの複雑なパスワードを登録すれば、それぞれのパスワードを覚えておく必要がなくなります。
また、カードにはパスワード（PIN）を設定することも可能ですので、その場合はカードの PIN だけを覚えれば認証できます。
詳しくは、『リファレンスガイド』の「機能編」－「Windows ログオン」、「アプリケーションログオン」をご覧ください。

■IC カード（FeliCa 方式）によるコンピュータのロック

IC カード（FeliCa 方式）をリーダ／ライタにセットした状態から外したり、リーダ／ライタにタッチしたりすることによって、コンピュータをロックすることができます。離席時にコンピュータをロックし、不正利用を防ぐための機能です。
詳しくは、『リファレンスガイド』の「機能編」－「Windows ログオン」－「カードのポーリング動作」をご覧ください。

■カード管理リスト

IC カード（FeliCa 方式）の属性を集中管理します。
IC カード（FeliCa 方式）紛失時などに、IC カード（FeliCa 方式）の無効化設定を行い、不正利用を防ぐ機能です。
詳しくは、『リファレンスガイド』の「機能編」－「カード監査」－「カード管理」をご覧ください。

運用上のご注意

SMARTACCESS では、外付けの FeliCa 対応リーダ／ライタ（PaSoRi）はサポートしておりません。

■ FeliCa 対応非接触 IC カードについて

FeliCa 対応リーダ／ライタには、認証に使用するための IC カードは添付されていません。弊社純正品「FeliCa 対応非接触 IC カード（SMARTACCESS 専用）（FMFLC-C1）」を別途ご購入ください。
なお、FeliCa 対応非接触 IC カードは SMARTACCESS 専用のカードです。カードにフォーマットを追加することができないため、他のソフトウェアや入退室管理システムなどのサービスにはご使用できません。

■ 通常備えておくこと

コンピュータの修理や保守を行うと、SMARTACCESS の設定がリセットされることがあります。そのような場合に備えて、必ず SMARTACCESS の設定を定期的にバックアップするよう設定を行ってください。
バックアップファイルは、紛失しないよう注意して管理してください。
バックアップの手順については、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧ください。

■ コンピュータの修理や保守を依頼する場合

□ 修理前に必要な作業

SMARTACCESS の設定のバックアップ

『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧になり、バックアップを行います。

「SMARTACCESS による Windows ログオン」を使用しない設定に変更する

必ず「SMARTACCESS による Windows ログオン」の設定を解除してください。
「SMARTACCESS による Windows ログオン」の設定を解除していないと、修理や保守ができないことがあります。また、「SMARTACCESS による Windows ログオン」の設定を解除せずに、修理すると、Windows にログオンできなくなることがあります。
解除の手順は次のとおりです。

1. **SMARTACCESS をインストールしたときと同じアカウントで Windows にログオンします。**

2. **「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。**
   「環境設定」が表示されます。

3. **「設定項目一覧」から「ログオン認証」→「Windows ログオン」の順にクリックします。**

4 パスワードの自動生成を行っている場合は、パスワードの自動生成を「しない」に設定します。

パスワードの自動生成を行っていない場合は、手順 6 に進んでください。

5 次の手順で Windows パスワードを任意のパスワードに変更します。

1. 「スタート」ボタン→「コントロールパネル」の順にクリックします。
   「コントロールパネル」ウィンドウが表示されます。
2. 「ユーザー アカウント」をクリックします。
   「ユーザー アカウント」ウィンドウが表示されます。
3. パスワードを変更するアカウントをクリックします。
4. 「パスワードを変更する」をクリックします。

この後はメッセージに従って操作します。

6 「SMARTACCESS による Windows ログオン」の「使用しない」にチェックし、「OK」をクリックします。

詳しくは、『リファレンスガイド』の「機能編」－「Windows ログオン」をご覧ください。

□ 修理後に必要な作業

リストアする

『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧になり、リストアを行います。

「SMARTACCESS による Windows ログオン」を使用する設定に変更する

「SMARTACCESS による Windows ログオン」を使用していた場合は、『リファレンスガイド』の「機能編」－「Windows ログオン」をご覧になり、「SMARTACCESS による Windows ログオン」の設定を「する」に変更してください。

■ コンピュータ本体のリカバリを実行した場合

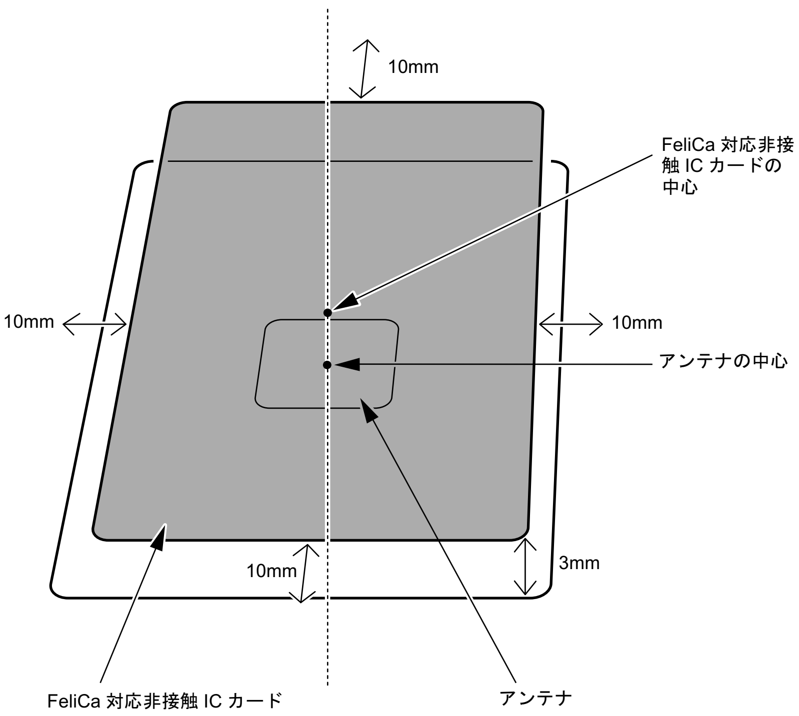
「Sony FeliCa リーダー／ライターソフトウェア」は再度インストールする必要があります。
「Sony FeliCa リーダー／ライターソフトウェア」のインストールについては、FeliCa 対応リーダ／ライタの「Readme.txt」（→ P.56）をご覧ください。

取り扱い方

コンピュータ本体に内蔵されているFeliCa対応リーダ／ライタは､鉄道の改札機などのリーダ／ライタと比べると電波強度が弱いため、FeliCa 対応非接触 IC カードを認識できる範囲が限られます。良好な通信が保証される範囲の目安は、次のとおりです（機種およびカードの種類によって若干異なります)。

・アンテナ表面からの距離は、3mm 以下

・FeliCa 対応非接触 IC カードの中心とアンテナの中心を合わせた状態から、前後左右に 10mm 以内



（イラストは機種により異なります）

重要

▶ お使いの機種によりアンテナの位置が異なります。アンテナの位置については、コンピュータ本体の『製品ガイド』の「各部名称」をご覧ください。

5 スマートカードリーダ／ライタ、スマートカードホルダー

接触型スマートカードに、ユーザー名やパスワード、証明書などのセキュリティ情報を格納します。このスマートカードをリーダ／ライタに差し込むことで、コンピュータ本体にセキュリティ情報を認識させます。離席時にはスマートカードを抜き取ることにより、不正利用を防止します。

セキュリティ機能の概要

■ログオン認証

Windows やソフトウェアなどの ID やパスワードをスマートカードに格納して、ログオン認証にスマートカードを使うことができます。
スマートカードを使ってログオンするときは、スマートカードに対するパスワード（PIN）を使用します。PIN を 1 つだけ覚えれば、複雑なパスワードをソフトウェアごとに覚える必要はありません。
詳しくは、『リファレンスガイド』の「機能編」－「Windows ログオン」、「アプリケーションログオン」をご覧ください。

■スマートカード抜き取りによるコンピュータのロック

離席時にスマートカードをリーダ／ライタから抜き取ることによってコンピュータをロックしたりシャットダウンしたりして、不正利用を防ぐことができます。
詳しくは、「運用例」－「スマートカードの抜き取りによるコンピュータのロック」（→ P.120）をご覧ください。

■スマートカードによる BIOS ロック

コンピュータの不正使用を防止するための BIOS のパスワード機能を、スマートカードと組み合わせて使用することができます。コンピュータの起動時やスタンバイからレジュームするときに、キーボードから BIOS パスワードを入力する代わりに、スマートカードをセットすることによって認証する機能です。
この機能は、スマートカードによる BIOS ロック機能に対応したコンピュータで使用可能です。
設定方法については「スマートカードによる BIOS ロックの設定」（→ P.39）をご覧ください。また、コンピュータ本体の BIOS 設定については、コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧ください。

スマートカードによる BIOS ロックの設定

スマートカードによる BIOS ロック機能をお使いになるには、コンピュータ本体の BIOS 設定を変更する必要があります。次の注意を参照し、正しく設定してください。
BIOS 設定の変更方法については、コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧ください。

重要

- スマートカードのPIN入力を連続して15回間違えて入力するとカードがロックされ使用できなくなります。
  ロックされたスマートカードではコンピュータにログオンできなくなるので PIN は忘れないようにしてください。
- BIOS ロック用パスワードを登録せずに本設定を行うと、コンピュータが起動できなくなります。

■注意事項

- スマートカードに BIOS ロック用パスワードを登録してから、BIOS の設定を変更してください。
  BIOS ロック用パスワードを登録せずに本設定を行うと、コンピュータが起動できなくなります。
- BIOS ロック用パスワードで使用できる文字は、半角英数字（a ～ z，A ～ Z，0 ～ 9）のみです。なお、スマートカードには大文字と小文字を区別して記録されますが、BIOS では大文字と小文字は区別されません。
  半角英数字以外の文字をお使いになると、コンピュータが起動できなくなります。
- BIOS ロック用パスワードは、1 枚のカードに 1 つのパスワードしか設定できません。
  BIOS で管理者用パスワードとユーザー用パスワードを別に設定した場合は、スマートカードを複数用意し、それぞれのパスワードを登録してください。
  ユーザー用パスワードの設定は、管理者用パスワード設定してからでないと行うことができません。
- スマートカードホルダーをお使いの場合、コンピュータ本体にスマートカードホルダーをセットしていないと、BIOS セットアップに「スマートカードによるロック」の項目は表示されません。
- SMARTACCESSで「管理者PIN」および「利用者PIN」を変更する場合は、1～16桁の半角英数字を使用してください。

■設定方法

□ スマートカードに BIOS ロック用パスワードを登録する

初めてスマートカードによる BIOS ロック機能をお使いになる場合は、次の手順に従って登録してください。

1 **BIOS ロック用パスワードを登録した管理者用スマートカード、利用者用スマートカードを作成する**

1. 管理者用スマートカード、利用者用スマートカードを作成する
   「インストールと設定」－「セキュリティ環境の構築」－「アカウントの登録」（→ P.77）をご覧になり、管理者用および利用者用スマートカードを作成します。管理者用スマートカードを作成した後、利用者用を作成してください。

2. スマートカードに BIOS ロック用パスワードを登録する
   詳しくは、『リファレンスガイド』の「ツール編」－「ユーザー情報設定」－「ログオン情報の登録」－「BIOS パスワード」をご覧ください。

2 コンピュータ本体の BIOS の設定を変更する

コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧になり、次の設定を行ってください。

1. BIOS セットアップの「管理者用パスワード」に管理者用スマートカードに登録した BIOS ロック用パスワードと同じパスワードを登録します。
2. 「ユーザー用パスワード」に利用者用スマートカードに登録した BIOS ロック用パスワードと同じパスワードを登録します。
3. スマートカードによるロックを使用する設定にします。

□ BIOS ロック用パスワードを変更する

スマートカードに登録した BIOS ロック用パスワードを変更する場合は、次の手順に従って変更してください。

1 コンピュータ本体の BIOS の設定を変更する

コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧になり、BIOS セットアップでスマートカードによるロックを使用しない設定にしてください。

2 管理者用スマートカードまたはユーザー用スマートカードの BIOS ロック用パスワードを変更する

変更方法については、『リファレンスガイド』の「ツール編」－「ユーザー情報設定」－「ログオン情報の登録」－「BIOS パスワード」をご覧ください。

運用上の注意

スマートカードをご購入の際は、「富士通パーソナル製品に関するお問合せ窓口」、またはご購入元にご連絡ください。

■通常備えておくこと

コンピュータの修理や保守を行うと、SMARTACCESS の設定がリセットされることがあります。そのような場合に備えて、必ず SMARTACCESS の設定を定期的にバックアップするよう設定を行ってください。
バックアップファイルは、紛失しないよう注意して管理してください。
バックアップの手順については、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧ください。

■コンピュータの修理や保守を依頼する場合

□ 修理前に必要な作業

SMARTACCESS の設定のバックアップ

『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧になり、バックアップを行います。

「SMARTACCESS による Windows ログオン」を使用しない設定に変更する

必ず「SMARTACCESS による Windows ログオン」の設定を解除してください。
「SMARTACCESS による Windows ログオン」の設定を解除していないと、修理や保守ができないことがあります。また、「SMARTACCESS による Windows ログオン」の設定を解除せずに、修理すると、Windows にログオンできなくなることがあります。
解除の手順は次のとおりです。

1 **SMARTACCESS をインストールしたときと同じアカウントで Windows にログオンします。**

2 **「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。**

「環境設定」が表示されます。

3 **「設定項目一覧」から「ログオン認証」→「Windows ログオン」の順にクリックします。**

4 **パスワードの自動生成を行っている場合は、パスワードの自動生成を「しない」に設定します。**

パスワードの自動生成を行っていない場合は、手順 6 に進んでください。

5 **次の手順で Windows パスワードを任意のパスワードに変更します。**

1. 「スタート」ボタン→「コントロールパネル」の順にクリックします。
   「コントロールパネル」ウィンドウが表示されます。
2. 「ユーザー アカウント」をクリックします。
   「ユーザー アカウント」ウィンドウが表示されます。
3. パスワードを変更するアカウントをクリックします。
4. 「パスワードを変更する」をクリックします。

この後はメッセージに従って操作します。

6 **「SMARTACCESS による Windows ログオン」の「使用しない」にチェックし、「OK」をクリックします。**

詳しくは、『リファレンスガイド』の「機能編」－「Windows ログオン」をご覧ください。

BIOS の設定を変更する

コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧になり、スマートカードによるロックを使用しない設定にします。

□ 修理後に必要な作業

リストアする

『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧になり、リストアを行います。

BIOS の設定を変更する

コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧になり、スマートカードによるロックを使用する設定にします。

「SMARTACCESS による Windows ログオン」を使用する設定に変更する

「SMARTACCESS による Windows ログオン」を使用していた場合は、『リファレンスガイド』の「機能編」－「Windows ログオン」をご覧になり、「SMARTACCESS による Windows ログオン」の設定を「する」に変更してください。

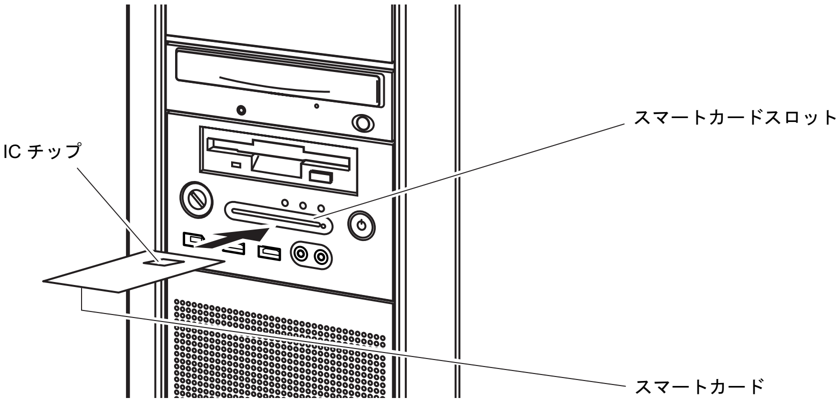
取り扱い方

■スマートカードリーダ／ライタ

スマートカードは IC チップ面を上にして、奥までゆっくり差し込みます。
スマートカードリーダ／ライタの位置などについては、コンピュータ本体の『製品ガイド』の「各部名称」をご覧ください。

POINT

- スマートカードリーダ／ライタにスマートカードを差し込むことによりコンピュータの電源を入れたり、スタンバイ状態からレジュームさせることができます。
  ただし、コンピュータの設定や、電源を切った状態によっては、電源が入らない場合があります。詳しくは、「取り扱い上の注意事項」－「スマートカードリーダ／ライタの注意事項」（→P.38）をご覧ください。

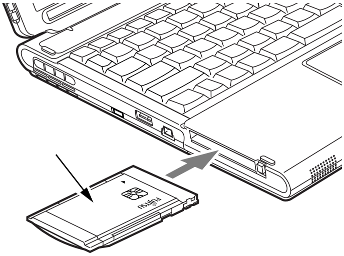


（イラストは機種や状況により異なります）

■スマートカードホルダー

□ スマートカードホルダーをセットする

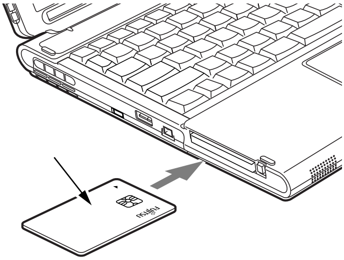
コンピュータ本体の電源が切れていること、スマートカードホルダーにスマートカードが差し込まれていないことを確認してから、「FUJITSU」のロゴがある面を上にして、コンピュータ本体のPCカードスロットにスマートカードホルダーをセットします。
PCカードスロットの位置や使い方については、コンピュータ本体の『製品ガイド』をご覧ください。



（イラストは機種や状況により異なります）

□ スマートカードをセットする

スマートカードはICチップ面を上にして、スマートカードホルダーの奥までゆっくり差し込みます。



（イラストは機種や状況により異なります）

□ スマートカードを抜き取る

スマートカードを使用するソフトウェアの指示に従うか、ソフトウェアが終了していることを確認してからスマートカードを抜き取ります。

重要

- スマートカードがソフトウェアを使用しているときにスマートカードを抜き取ると、データが破壊されるおそれがあります。必ずソフトウェアの抜き取り指示に従うか、ソフトウェアが終了していることを確認してから抜き取ってください。

□ スマートカードホルダーを取り出す

コンピュータ本体の電源を切り、PCカードスロットからスマートカードホルダーを取り出します。
PCカードスロットから取り出す方法については、コンピュータ本体の『製品ガイド』をご覧ください。

取り扱い上の注意事項

□ スマートカードリーダ／ライタの注意事項

- スマートカードをセットしている状態からコンピュータを再起動するときは、「OK」または「はい」をクリックして再起動を実行してから、起動画面が出るまでの間に、スマートカードを取り出してください。
- コンピュータを正常にシャットダウンした場合、およびスタンバイ状態のときにスマートカードをセットすると、コンピュータに電源が入ったりレジュームしたりします。

□ スマートカードホルダーの注意事項

- スマートカードホルダーは、コンピュータ本体の電源が入った状態でのセットまたは取り出しに対応しておりません。必ず、コンピュータ本体の電源を切った状態で行ってください。
- スマートカードホルダーをセットしたり取り出したりする場合は、必ずスマートカードを取り出しておいてください。
- スマートカードホルダーは、他のスマートカード読み取り装置と同時に使用することはできません。
- スマートカードホルダーは、IC チップを使用した大変デリケートな電子部品です。
  落下などの衝撃を与えないでください。
- スタンバイや休止状態からレジューム（復帰）後、もう一度スタンバイや休止状態を行う場合は、しばらく（30 秒程度）待ってから操作してください。短い間隔で行うと、正しく動作しない場合があります。

□ 共通の注意事項

- スマートカードを使用するときは、次の点に注意してください。
  - 折り曲げたり、汚したり、濡らしたりしないでください。
  - 磁石などの磁気を帯びたものを近づけないでください。
  - 電気を帯びたものを上に載せたり、近くで静電気を発生させたりしないでください。
  - 高温の場所に保管しないでください。
  - カードに衝撃を与えないでください。
- コンピュータを持ち運ぶ場合は、スマートカードを取り出しておいてください。
- 他の装置で作成した、拡張情報の多いスマートカードの読み取りを行うと、ごくまれにスマートカードの機能が停止する場合があります。
  このような場合、コンピュータを再起動してください。再起動後、スマートカードリーダ／ライタやスマートカードホルダーで作成したスマートカードをお使いになるか、拡張情報を減らした形式で作成し直したスマートカードをお使いください。
- 寿命について
  スマートカードは、カードに搭載されている IC チップを、スマートカードリーダ／ライタやスマートカードホルダー内部のソケットに接触させることによって、IC チップに内蔵されている情報の読み取り／書き込みを行います。そのため、同じスマートカードホルダー、スマートカードを長期間にわたって使用していると、IC チップやソケットなどの電子部品が消耗して、正しい情報の読み取り／書き込みができなくなってきます。保守作業として定期的にスマートカードホルダー、スマートカードを交換することをお勧めします。
  なお、次の状態になった場合を交換の目安としてください。

- スマートカードをセットしても認識されなくなってきた場合
- スマートカードが読み取りにくくなってきた場合
- データの更新に時間がかかるようになってきた場合

Memo

3

第 3 章

SMARTACCESS の機能概要

SMARTACCESSには、不正アクセスや情報漏えいへの対策として、複数の認証デバイスを使ったログオン認証、不正デバイスの使用防止などの機能があります。
この章では、SMARTACCESSの主な機能について説明しています。

1 セキュリティ対策

使用する権限のない人に不正にコンピュータを使われて、データが破壊されたり漏えいしたりする危険からコンピュータを守ることが必要になってきています。SMARTACCESS では不正使用対策や情報漏えい対策として、指紋センサーや静脈センサーによる本人認証や、セキュリティチップによるデータ保護、カードによるログオン情報の保護ができます。複数の認証デバイスを組み合わせることによって、コンピュータの安全性をより高めることができます。

不正使用対策

■ Windows ログオン

Windows の起動時やコンピュータのロック、休止状態からの復帰、スクリーンセーバーからの復帰時に入力するユーザー名、パスワードを認証デバイスに設定できます。これにより、悪意のある第三者によって不正に Windows にログオンされることを防ぎます。複数の認証デバイスを組み合わせて使用すれば、パスワードを入力するだけの認証よりもさらにセキュリティが高まります。
詳しくは「インストールと設定」－「セキュリティ環境の構築」－「Windows ログオンの設定」（→ P.85）をご覧ください。

■ アプリケーションログオン

ユーザー名とパスワードで運用している Web サイトやソフトウェアなどのセキュリティレベルを強化します。
パスワード認証を必要とするソフトウェアや Web サイトをあらかじめ登録しておくと、暗号化して認証デバイスに登録されているユーザー名やパスワードを利用してソフトウェアにログオンします。
認証デバイスにユーザー情報を格納したり、ユーザー情報と関連付けたりすることによって、パスワードを入力するだけの認証よりもさらにセキュリティが高まります。
詳しくは「インストールと設定」－「セキュリティ環境の構築」－「アプリケーションログオンの設定」（→ P.86）をご覧ください。

情報漏えい対策

■ Windows 暗号化ファイルシステム（EFS）の鍵をセキュリティチップで保護

ハードディスクに保存されているファイルをより強固に守ります。
Windows でファイルとフォルダの暗号化を設定することにより、暗号化に利用される鍵をセキュリティチップで安全に管理します。
暗号鍵がハードディスクに保管されていないため、ハードディスクを盗まれた場合でも、暗号鍵を解析されて暗号化した機密文書が漏えいしてしまうのを防ぎます。
詳しくは「運用例」－「セキュリティチップで暗号化ファイルの鍵を保護する」（→ P.112）をご覧ください。

■ 機器監査

あらかじめ機器構成を登録して Windows 起動時に機器監査を行い、第三者によって登録外の機器構成に変更された場合にログオンを拒否できます。これにより使用者の意図しない不正なハードウェアが取り付けられることを防ぎます。
セキュリティチップを搭載したコンピュータでお使いになれます。
詳しくは、「認証デバイスについて」－「セキュリティチップ」－「セキュリティ機能の概要」－「コンピュータの不正なハードウェアの変更の検出」（→ P.15）をご覧ください。

■ 機器制限

USB や光学ドライブ、シリアル、パラレル、赤外線通信などの各ポートの使用を制限して不正なハードウェアが取り付けられることを防ぎます。これによりコンピュータからの重要データの持ち出しを未然に防ぎます。
この機能は Portshutter や FENCE-G と連携することでお使いになれます。
FENCE-G との連携機能をお使いになるには、SMARTACCESS/Premium が必要です。
詳しくは『リファレンスガイド』の「機器制限」をご覧ください。

2 運用管理機能

SMARTACCESS には、運用管理機能として「利用ログ管理」機能や「バックアップツール」があります。また、SMARTACCESS の運用を統合化するために Systemwalker や Active Directory との連携機能があります。

セキュリティイベントの監査

システムで発生したエラーや警告などのログ情報をログファイルに格納します。コンピュータ上で不正アクセスの原因や利用状況などを追跡できます。
また、Systemwalker と連携することができます。これにより、ログオン情報を一元管理して管理画面からリアルタイムに状況を把握することが可能になります。例えば、ログオンを何回も失敗しているユーザーがいるといった異常な状態を、リアルタイムで把握できます。この機能をお使いになるには、SMARTACCESS/Premium が必要です。

障害からの復旧

ファイル装置や認証デバイスなどの障害による SMARTACCESS の環境設定情報やユーザー情報の損失に備え、バックアップファイルを作成します。また、障害により環境設定情報やユーザー情報を損失した場合は、バックアップファイルから復元できます。

ネットワーク管理

企業規模がある程度以上になると、全社規模でのコンピュータのセキュリティ管理が重要になってきます。それぞれのコンピュータで管理していた認証用の情報や SMARTACCESS の利用環境の情報をネットワークレベルで集中管理することができます。
バイオ認証装置と連携することで、指紋などの認証用の情報をバイオ認証装置で一元管理でき、さらにバイオ認証を行うことができます。
また、Windows ドメイン環境では、Active Directory と連携した運用ができます。SMARTACCESS の利用環境をドメイン内で標準化して管理することができます。この機能をお使いになるには、SMARTACCESS/Premium が必要です。

4

第 4 章

インストールと設定

各認証デバイスを使ったセキュリティ対策機能などをお使いになるには、認証デバイスおよびSMARTACCESSのインストール、利用するセキュリティ環境にあったセットアップが必要です。
この章では、認証デバイスやSMARTACCESSの導入からお使いになるまでの基本的な流れを説明しています。

1 導入モデル

SMARTACCESS は、スタンドアロンまたはワークグループ環境、ドメイン環境で、認証デバイスを利用するセキュリティ環境を構築できます。また、セキュリティ環境を構築する側、セキュリティ環境を利用する側、それぞれで SMARTACCESS の使用権限が異なります。

SMARTACCESS での管理者と利用者

SMARTACCESS を使ったセキュリティ環境を構築する側を「管理者」、そのセキュリティ環境を利用する側を「利用者」と呼びます。
管理者は最適なセキュリティ環境を利用者に提供するための設定および管理を行い、利用者はそのセキュリティ環境により認証デバイスを利用してコンピュータに安全にアクセスすることができます。

管理者および利用者の権限は次のとおりです。

	スタンドアロンまたはワークグループ環境	ドメイン環境
管理者	ローカルコンピュータのAdministratorsグループのメンバー	ActiveDirectory（ドメインコントローラ）のDomain Adminsグループのメンバー
利用者	Usersグループのメンバー	Domain Usersグループのメンバー

運用形態

SMARTACCESS の主な運用形態は次のとおりです。

■1 台のコンピュータで管理者と利用者が同一の運用

導入から環境の設定、利用するまでを一括して一人で行います。主に個人ユーザーが利用する場合の運用形態です。

■1 台のコンピュータで管理者と利用者が異なる運用

導入から環境の設定まで、一連の構築を管理者が行います。利用者は管理者が構築した環境で SMARTACCESS を利用します。

■1 台のコンピュータを複数の利用者が使う運用

複数の利用者が 1 台のコンピュータを共有して使う場合、導入から利用者ごとの環境の設定までを管理者が行います。利用者は利用者ごとに設定された環境で SMARTACCESS を利用します。

■ネットワーク運用

バイオ認証装置やActiveDirectoryと連携し､1台のコンピュータが認証用の情報やSMARTACCESSの環境設定情報を一括して管理します。利用者はスタンドアロンまたはワークグループ環境と同等にお使いになれます。
ネットワーク運用については、「ネットワーク運用」(→ P.127)をご覧ください。

重要

- バイオ認証装置や Active Directory との連携機能をお使いになるには、SMARTACCESS/Premium が必要です。

2 作業の流れ

導入の手順は、お使いになる認証デバイスやセキュリティ環境によって異なります。主な手順は次のとおりです。

□ 用意するもの

- パソコンまたはワークステーション本体
- ドライバーズディスク(SMARTACCESS/Basic の場合)、または「SMARTACCESS/Premium」CD-ROM

インストールと設定の作業の流れは次のとおりです。

1 認証デバイスのインストール(→ P.55)

2 SMARTACCESS のインストール(→ P.58)

3 SMARTACCESS の設定

- **認証パターンの登録の確認(→ P.74)**
- **アカウントの登録(→ P.77)**
- **Windows ログオンの設定(→ P.85)**
  必要に応じて行います。
- **アプリケーションログオンの設定(→ P.86)**
  必要に応じて行います。
- **認証用のユーザー情報の登録(→ P.94)**
  指紋センサー、および静脈センサーをお使いになる場合は登録が必須です。
- **ポリシーの設定**
  必要に応じて行います。ポリシーについては、『リファレンスガイド』の「ツール編」－「環境設定」－「ポリシー」をご覧ください。
- **ログオン認証(シングルサインオン、機器監査など)の設定**
  必要に応じて行います。ログオン認証については、『リファレンスガイド』の「機能編」－「ログオン認証」をご覧ください。
- **機器制限の設定**
  必要に応じて行います。機器制限については、『リファレンスガイド』の「機能編」－「機器制限」をご覧ください。
- **運用管理(連携、利用ログ)の設定**
  必要に応じて行います。
  この機能をお使いになるには、SMARTACCESS/Premium が必要です。
  - Windows Server の Active Directory との連携については、『リファレンスガイド』の「機能編」－「Active Directory 連携」をご覧ください。
  - バイオ認証装置との連携については、『リファレンスガイド』の「機能編」－「バイオ認証装置連携」をご覧ください。
  - 利用ログについては、『リファレンスガイド』の「機能編」－「利用ログ」をご覧ください。

3 認証デバイスのインストール

SMARTACCESS をインストールする前に、お使いになる認証デバイスのドライバやユーティリティソフトのインストールが必要です。SMARTACCESS では、複数の認証デバイスを組み合わせて利用することもできます。

BIOS の設定を変更または確認する

次の認証デバイスをお使いになる場合、認証デバイスのドライバやユーティリティソフトをインストールする前に必ず BIOS の設定を変更してください。
・セキュリティチップ
・FeliCa 対応リーダ／ライタ

□ セキュリティチップをお使いになる場合

コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧になり、BIOS の設定を変更してください。

□ FeliCa 対応リーダ／ライタをお使いになる場合

コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧になり、BIOS の設定を変更してください。

認証デバイスのインストール

認証デバイスのドライバやユーティリティソフトのインストールの主な流れは次のとおりです。
詳しくは、それぞれの認証デバイスの「Readme.txt」（→ P.56）をご覧ください。

□ セキュリティチップをお使いになる場合

セキュリティチップと他の認証デバイスと組み合わせてお使いになる場合も含みます。

1 Security Platform のインストール

認証デバイスとしてセキュリティチップだけをお使いになる場合は、これでインストールが完了です。

2 ドライバのインストール

セキュリティチップと他の認証デバイスを組み合わせてお使いになる場合、Security Platform をインストールしてから他の認証デバイスのドライバをインストールします。

□ セキュリティチップ以外の認証デバイスをお使いになる場合

1 ドライバのインストール

■「Readme.txt」の格納先

□ SMARTACCESS/Premium の場合

「SMARTACCESS/Premium」CD-ROM の、次のフォルダ内に格納されています。

認証デバイス		格納先フォルダ
指紋センサー	指紋センサー	¥fingerprint
	指紋認識エンジン	¥FSTDrv
セキュリティチップ		¥IFXSW20
FeliCa 対応リーダ／ライタ		¥SONY FeliCa リーダー _ ライター

注：・スマートカードをお使いになる場合、「SMARTACCESS/Premium」CD-ROM にはスマートカード用のドライバが格納されておりません。
　　お使いのコンピュータに添付の「ドライバーズディスク」（→ P.56）をご覧ください。
　・静脈センサーをお使いになる場合、「SMARTACCESS/Premium」CD-ROM には静脈センサー用のドライバが格納されておりません。
　　「手のひら静脈認証装置 取扱説明書 CD」をご覧ください。

□ SMARTACCESS/Basic の場合

「ドライバーズディスク」の、次のフォルダ内に格納されています。

認証デバイス		格納先フォルダ
指紋センサー（FMV-LIFEBOOK）	指紋センサー	¥Other¥fingerprint
	指紋認識エンジン	¥Other¥FSTDrv
セキュリティチップ		¥Other¥IFXSW20
スマートカードリーダ／ライタ（FMV-ESPRIMO、CELSIUS シリーズ）		¥Other¥Smart
スマートカードホルダーまたはスマートカードスロット（FMV-LIFEBOOK）		¥Other¥O2scb2kxp

重要

- 認証デバイスをインストールするときは、管理者権限で Windows にログオンする必要があります。
- 認証デバイスをインストールする前には、使用中のソフトウェアをすべて終了させてください。
- スマートカードをお使いになる場合、ドライバのインストール後に次の手順でスマートカードの設定を確認してください。
  1. 「スタート」ボタン→「コントロールパネル」の順にクリックします。
     「コントロールパネル」ウィンドウが表示されます。
  2. 「パフォーマンスとメンテナンス」→「管理ツール」→「サービス」の順にクリックします。
     「サービス」ウィンドウが表示されます。
  3. 「Smart Card」の「スタートアップの種類」が「自動」になっていることを確認します。
     「スタートアップの種類」が「自動」になっていない場合は次の手順に進みます。
     「自動」になっている場合は、確認はこれで完了です。

4. 「Smart Card」をダブルクリックします。
   「（ローカル コンピュータ）Smart Card のプロパティ」ウィンドウが表示されます。
5. 「全般」タブの「スタートアップの種類」から「自動」を選択します。
6. 「OK」をクリックし、すべてのウィンドウを閉じます。

4 SMARTACCESS のインストール

認証デバイスのインストール完了後、コンピュータが再起動してから、SMARTACCESS をインストールします。

準備

□ SMARTACCESS をインストールする前に

あらかじめ次のことを確認してください。

・SMARTACCESS は Windows ログオン認証を行うソフトウェアと併用することができません。SMARTACCESS をインストールする場合は、必ず他の Windows ログオン認証ソフトウェアをアンインストールしてください。

□ Windows 2000 をお使いの場合

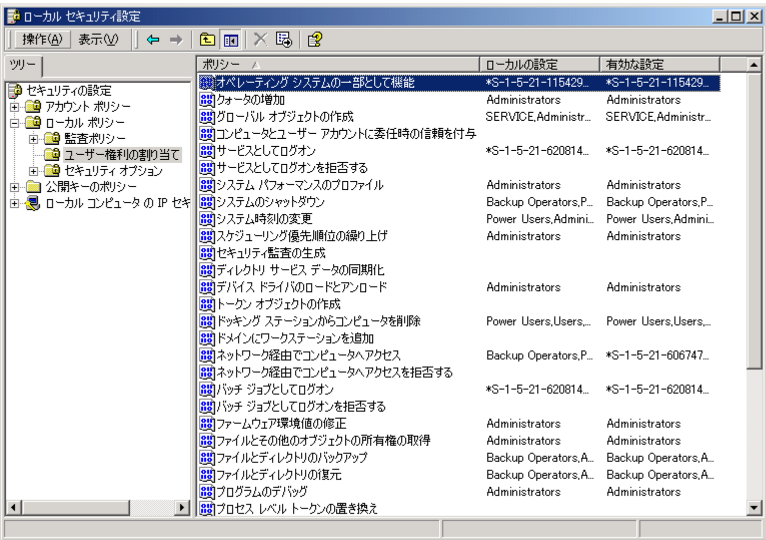
Windows 2000 をお使いの場合、「ユーザー権利の割り当て」の設定を変更する必要があります。SMARTACCESS をインストールするには、Windows アカウントの管理者権限を持つユーザーである必要があります。

1 「スタート」ボタン→「コントロールパネル」の順にクリックします。

「コントロールパネル」ウィンドウが表示されます。

2 「パフォーマンスとメンテナンス」→「管理ツール」→「ローカル セキュリティ ポリシー」の順にクリックします。

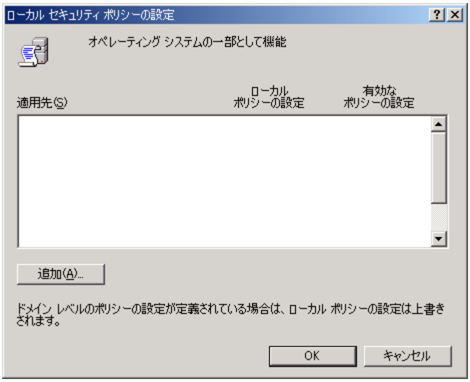
「ローカル セキュリティ設定」が起動します。



3 **ツリーから「ローカル ポリシー」→「ユーザー権利の割り当て」の順にクリックします。**

4 **ポリシーから「オペレーティングシステムの一部として機能」をダブルクリックします。**

「ローカル セキュリティ ポリシーの設定」ウィンドウが表示されます。

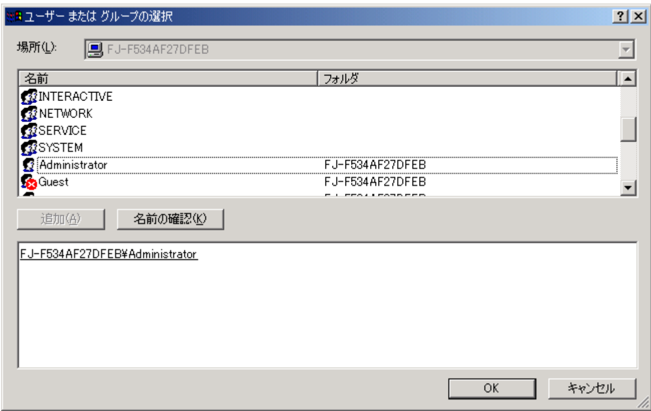


5 **「追加」をクリックします。**

「ユーザーまたはグループの選択」ウィンドウが表示されます。

6 **名前から管理者権限のユーザーまたはグループを選択して「追加」をクリックします。**

選択した管理者がウィンドウ下側に表示されます。



7 **「OK」をクリックして、「ローカル セキュリティ ポリシーの設定」ウィンドウに戻ります。**

8 **適用先一覧に手順 6 で選択したアカウントが追加されことを確認し、「OK」をクリックします。**

「ローカル セキュリティ設定」ウィンドウに戻ります。

9 **「ファイル」→「終了」の順にクリックします。**

「ローカルセキュリティ設定」が終了します。

10 **コンピュータを再起動して、設定を有効にします。**

重要

- 「ローカルセキュリティ設定」については、Windows2000 のヘルプをご覧ください。

SMARTACCESS のインストール

□ インストールの権限について

SMARTACCESSをインストールするには、Windowsアカウントの管理者権限を持つユーザーである必要があります。
運用形態とインストールする管理者権限の関係は、次のとおりです。

運用形態	必要とする権限
スタンドアロンまたはワークグループ環境	ローカルコンピュータの Administrators グループのメンバー
ドメイン環境	ActiveDirectory（ドメインコントローラ）の Domain Admins グループのメンバー

□ SMARTACCESS のインストール

SMARTACCESS のインストールは、インストーラを実行して画面の指示に従いながら行います。
次の手順でインストールを行ってください。

重要

- お使いになる認証デバイスのインストールが完了してから、SMARTACCESS をインストールしてください。SMARTACCESS をインストールした後に認証デバイスをインストールすると、認証デバイスが正常に認識されません。
- スマートカードホルダーをお使いになる場合、スマートカードホルダーを取り付けた状態で SMARTACCESS をインストールしてください。
  スマートカードホルダーの取り付け方については、「認証デバイスについて」「スマートカードホルダー」－「使い方」（→ P.43）をご覧ください。
- SMARTACCESS をインストールする前に、使用中のソフトウェアはすべて終了させてください。
- ハードディスクに十分な空き容量（→ P.10）があることを確認してください。

1 **次のディスクをセットします。**

- SMARTACCESS/Premium の場合
  「SMARTACCESS/Premium」CD-ROM
- SMARTACCESS/Basic の場合
  パソコンまたはワークステーション本体に添付の「ドライバーズディスク」

2 **「スタート」ボタン→「ファイル名を指定して実行」の順にクリックします。**

3 「名前」に次のように入力し、「OK」をクリックします。

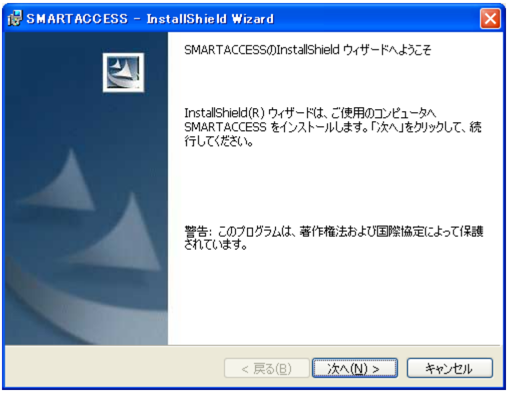
・SMARTACCESS/Premium の場合

[CD/DVD ドライブ]:¥SAPremium¥Setup¥setup.exe

・SMARTACCESS/Basic の場合

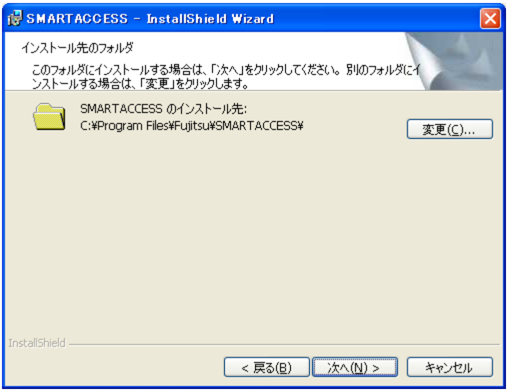
[CD/DVD ドライブ]:¥Other¥SABasic¥Setup¥setup.exe

「SMARTACCESS 用の InstallShield ウィザードへようこそ」と表示されます。



4 「次へ」をクリックします。

「インストール先のフォルダ」が表示されます。



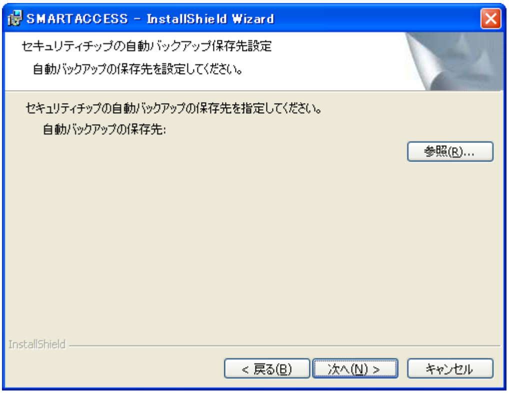
5 インストール先を確認し、「次へ」をクリックします。

インストール先を変更する場合は、「変更」をクリックします。

■ セキュリティチップがインストールされている場合

「セキュリティチップの自動バックアップ保存先設定」ウィンドウが表示されます。

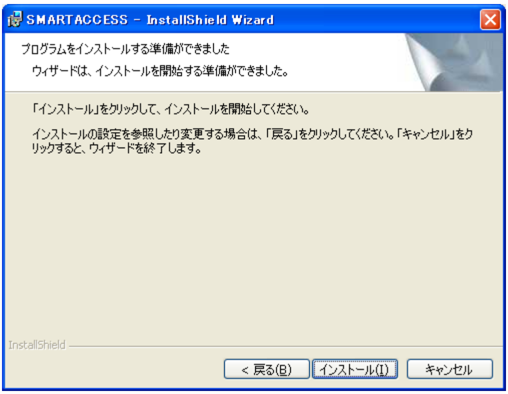
手順 6 に進んでください。



■ セキュリティチップがインストールされていない場合

「プログラムをインストールできる準備ができました」と表示されます。

手順 9 に進んでください。

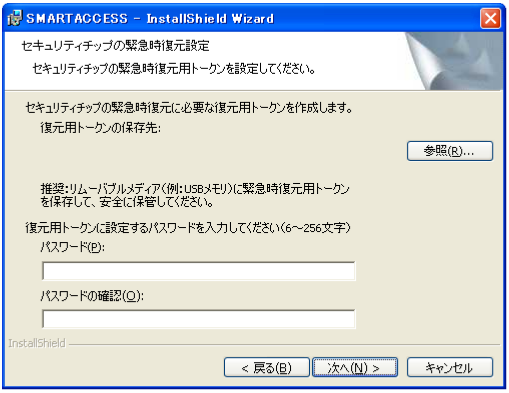


POINT

- セキュリティチップをお使いになる場合、システムフォルダのあるドライブと、SMARTACCESS のインストール先ドライブは同じ場所にしてください。セキュリティチップが正常に使用できなくなる場合があります。

6 「参照」をクリックして、自動バックアップの保存先を指定します。

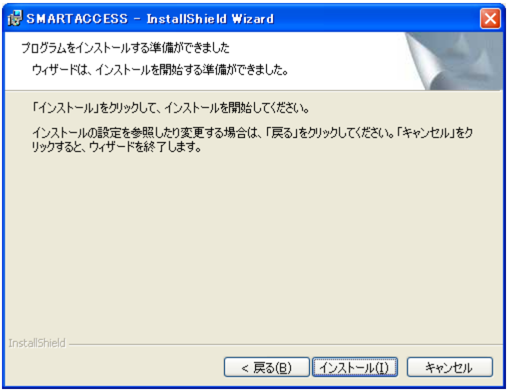
「セキュリティチップの緊急時復元設定」ウィンドウが表示されます。



7 「参照」をクリックして、復元用トークンの保存先を指定します。

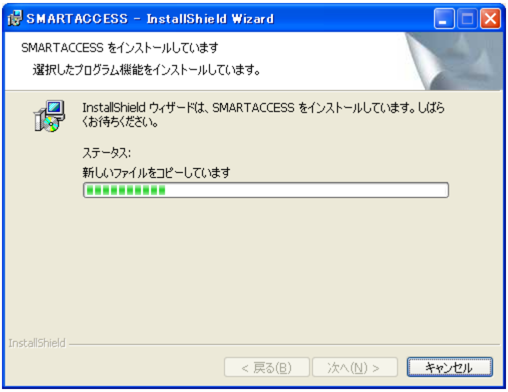
8 「パスワード」と「パスワードの確認」に、復元用トークンに設定するパスワードを 6 文字以上 256 文字以下で入力します。

「プログラムがインストールできる準備ができました」と表示されます。

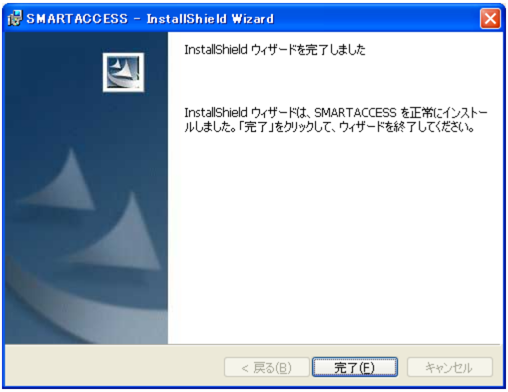


9 「インストール」をクリックして、インストールを開始します。

「SMARTACCESS をインストールしています」と表示されます。

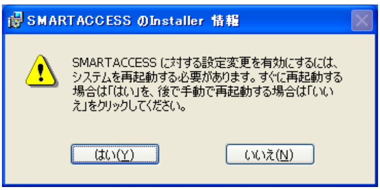


インストールが正常に完了すると、「InstallShield ウィザードを完了しました」と表示されます。



10 「完了」をクリックします。

「SMARTACCESS の InstallShield 情報」メッセージが表示されます。



重要

- インストールの完了後に、「コマンドプロンプト」ウィンドウが表示されることがあります。「コマンドプロンプト」ウィンドウは自動的に閉じますので手動で終了しないでください。

11 「はい」をクリックして、コンピュータを再起動します。

SMARTACCESS のインストール情報を有効にするには、Windows の再起動が必要です。

重要

- セキュリティチップをお使いになる場合、SMARTACCESS インストール後に「最近使ったファイル」の一覧に、自動バックアップの保存先で指定したファイルと復元用トークンの保存先で指定したファイルが追加されることがありますが、選択しないでください。

認証デバイスの追加

SMARTACCESS/PremiumV1.1L21、または SMARTACCESS/BasicV1.1L21 をすでに導入している環境に認証デバイスを追加する場合は、SMARTACCESS/PremiumV1.1L21、または SMARTACCESS/BasicV1.1L21 をインストールし直す必要があります。

1 「バックアップツール」で、環境設定情報や全ユーザーのデータを退避します。

「バックアップツール」については、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧ください。

2 SMARTACCESS をアンインストールします。

詳しくは、「アンインストール」－「SMARTACCESS のアンインストール」(→ P.109) をご覧ください。

3 追加する認証デバイスのドライバやユーティリティソフトをインストールします。

詳しくは、「認証デバイスのインストール」(→ P.55) をご覧ください。

4 SMARTACCESS をインストールします。

詳しくは、「SMARTACCESS のインストール」(→ P.60) をご覧ください。

5 「バックアップツール」で、環境設定情報や全ユーザーのデータを復元します。

詳しくは、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」－「バックアップファイルの復元」をご覧ください。

重要

- 認証デバイスとして指紋がインストールされている環境に、静脈の認証デバイスを追加することはできません。また認証デバイスとして静脈がインストールされている環境に、指紋の認証デバイスを追加することはできません。
- 「バックアップツール」によるデータの復元後は、「認証パターン」の設定は前の環境の設定が引き継がれるため、追加した認証デバイスをそのまま使用することはできません。追加した認証デバイスをお使いになる場合は、「認証パターン」を設定し直してください。
  「認証パターン」の設定については、『リファレンスガイド』の「ツール編」－「環境設定」－「ログオン認証」をご覧ください。
- 「バックアップツール」により指紋や静脈の個別ユーザー情報は退避されません。指紋や静脈の「運用モード」で「パーソナル運用モード」を使用時に「認証デバイスの追加」を実行する場合は、データの退避を実行する前に必ず「通常運用モード」または「モバイル運用モード」で「個別ユーザー情報を使用」を「しない」に設定してください。「パーソナル運用モード」に設定を戻す場合は、データの復元後に個別ユーザー情報を取得し直してから、「パーソナル運用モード」に変更してください。
  「運用モード」の設定については、『リファレンスガイド』の「ツール編」－「環境設定」－「ポリシー」－「指紋」または「静脈」をご覧ください。

5 SMARTACCESS のツール

SMARTACCESS のインストールが完了すると、「環境設定」と「ユーザー情報設定」の 2 つのツールがお使いになれます。
詳しくは、『リファレンスガイド』の「ツール編」をご覧ください。

環境設定

「環境設定」は、管理者が SMARTACCESS を利用するセキュリティ環境の設定を管理するためのツールです。
「環境設定」で設定する機能は次のとおりです。

■ログオン認証

Windows ログオン、アプリケーションログオンおよび認証パターンなどの設定をします。

□ 対象製品

・SMARTACCESS/Premium
・SMARTACCESS/Basic

■ポリシー

SMARTACCESS ツールの起動制限や認証デバイスごとのセキュリティ設定をします。

□ 対象製品

・SMARTACCESS/Premium
・SMARTACCESS/Basic

■機器制限

Portshutter や FENCE-G（SMARTACCESS/Premium のみ）の設定をします。

□ 対象製品

・SMARTACCESS/Premium
・SMARTACCESS/Basic

■連携

ActiveDirctory や Systemwalker との連携を設定します。

□ 対象製品

・SMARTACCESS/Premium

■利用ログ管理

ログ取得に関する設定をします。

□ 対象製品

・SMARTACCESS/Premium

■ユーザー情報管理

アカウントおよび認証情報の登録や管理をします。

□ 対象製品

・SMARTACCESS/Premium
・SMARTACCESS/Basic

ユーザー情報設定

「ユーザー情報設定」は、指紋などの情報やパスワードなど、利用者固有の設定を利用者自身が設定するためのツールです。
「ユーザー情報設定」で設定する機能は次のとおりです。

■ログオン情報の登録

BIOS、Windows、およびアプリケーションのログオン情報を登録したり変更したりします。

□ 対象製品

・SMARTACCESS/Premium
・SMARTACCESS/Basic

■証明書

スマートカードの証明書を登録します。

□ 対象製品

・SMARTACCESS/Premium
・SMARTACCESS/Basic

■連携

連携認証情報を登録したり変更したりします（「環境設定」から「ユーザー情報設定」を起動した場合に表示されます）。
FENCE-G や Systemwalker との連携情報を登録したり変更したりします（「環境設定」で、FENCE-G や Systemwalker を利用する設定をした場合に表示されます）。
FENCE-G と Systemwalker との連携機能は、SMARTACCESS/Premium の場合にお使いになれます。

□ 対象製品

・SMARTACCESS/Premium
・SMARTACCESS/Basic

■ユーザー情報の管理

利用者のアカウント、および認証情報を登録したり変更したりします。

□ 対象製品

・SMARTACCESS/Premium
・SMARTACCESS/Basic

SMARTACCESS をお使いになる前に

■Windows アカウントのパスワード設定

SMARTACCESS の管理者および利用者には、Windows アカウントにパスワード設定が必要です。
既存の Windows アカウントを SMARTACCESS でお使いになる場合は、あらかじめ Windows でパスワードの設定をします。
新規に Windows アカウントを作成する場合は、SMARTACCESS の「環境設定」で Windows アカウントとパスワードの設定ができます（→ P.77）。

重要

▶ Windows のパスワード設定については、Windows のヘルプをご覧ください。

■ご購入時の設定について

認証デバイスには、ご購入時にユーザー名やパスワード、PIN があらかじめ設定されていますが、セキュリティ上、使い始めるときには必ずパスワードや PIN を変更してください。パスワードや PIN の変更については、『リファレンスガイド』の「ツール編」－「環境設定」－「ユーザー情報管理」、または「ユーザー情報設定」－「ユーザー情報管理」をご覧ください。

認証デバイスのご購入時の設定は次のとおりです。

認証デバイス	設定項目	ご購入時の設定
セキュリティチップ	所有者パスワード	administrator
指紋センサー	指紋ユーザー名	saadmin
指紋センサー	バイオパスワード	administrator
IC カード（FeliCa 方式）	利用者 PIN	0000 注
IC カード（FeliCa 方式）	管理者 PIN	administrator 注
スマートカード	利用者 PIN	0000 注
スマートカード	管理者 PIN	administrator 注

注：FMV オプション製品である FeliCa 対応非接触 IC カード（FMFLC-C1）およびスマートカード（FMSMA-C1）を使用した場合の設定値です。それ以外のカードで作成や発行を行った場合はこの限りではありません。

重要

▶ すでにセキュリティチップの所有者パスワードが設定されている場合、設定されている所有者パスワードが有効になります。

■Windows XP の「共有とセキュリティ」をお使いの場合

Windows XP の「共有とセキュリティ」を使って、ユーザープロファイルのフォルダを「プライベート」に設定している場合は、ユーザープロファイルのフォルダへのアクセスは利用者のみに許可されます。
SMARTACCESS の設定を行うとき、管理者が利用者のユーザープロファイルのフォルダにアクセスする必要があることがありますので、「このフォルダをプライベートにする」の設定をオフにしてください。
設定をオフにする手順は次のとおりです。

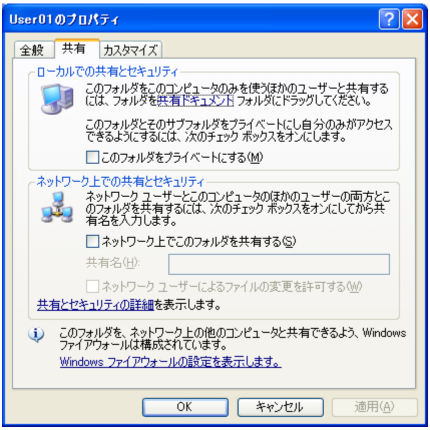
重要

- 「このフォルダをプライベートにする」設定を変更するには、管理者権限をもつアカウントでログオンしている必要があります。
- ユーザープロファイルやフォルダのプライベート設定については、Windows のヘルプをご覧ください。

1 **「スタート」ボタン→「マイコンピュータ」の順にクリックします。**
「マイコンピュータ」ウィンドウが表示されます。

2 **Windows がインストールされているドライブ（通常は「ローカル ディスク（C:)」）→「Document and Settings」の順にダブルクリックします。**

3 **設定を変更するユーザーアカウント名のフォルダを右クリックし、「共有とセキュリティ」をクリックします。**
「[ユーザー名］のプロパティ」ウィンドウが表示されます。



「このフォルダをプライベートにする」のチェックを外します。

4 **「OK」をクリックし、すべてのウィンドウを閉じます。**

重要

- 運用上の都合などで「このフォルダをプライベートにする」をチェックしている場合、管理者は次の設定ができなくなります。
  ・「環境設定」－「ユーザー情報管理」の「アカウント追加」

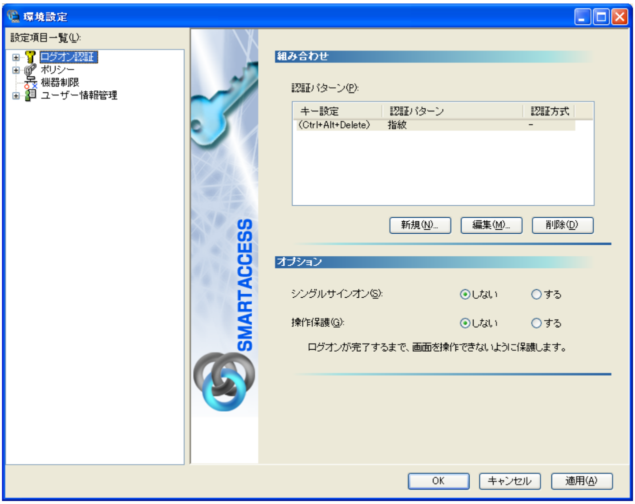
- 「環境設定」－「ユーザー情報管理」－「セキュリティチップ」の「ユーザー情報設定の起動」
- 「ユーザー情報設定」

環境設定の起動

「環境設定」を起動するには、SMARTACCESS をインストールした管理者権限をもつアカウントで Windows にログオンする必要があります。

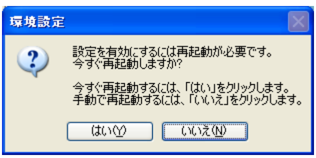
1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。

「環境設定」が起動します。
左側の、機能をツリー構造で表示している領域を「設定項目一覧」と呼び、右側には「設定項目一覧」から選択した機能の設定内容を表示します。
「設定項目一覧」には、導入されてない認証デバイスや、インストールされていない連携ソフトウェアは表示されません。また、設定内容にはコンピュータ全体の設定が表示されます。



POINT

- 「設定項目一覧」から選択した機能を設定したら「適用」をクリックし、続けて他の機能を設定することができます。
- 「環境設定」を終了するには、「OK」をクリックします。設定を変更した場合は再起動が要求されることがあります。その場合、再起動することで設定を有効にすることができます。



ユーザー情報設定の起動

「ユーザー情報設定」では利用者自身の設定内容の確認や設定を行います。

重要

- 「環境設定」で設定されている認証デバイスによる認証が要求されます。
「ユーザー情報設定」をお使いになる前に、必ず「セキュリティ環境の構築」（→ P.74）の手順に従って、「環境設定」で利用者のアカウントと認証情報を登録してください。

1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「ユーザー情報設定」の順にクリックします。

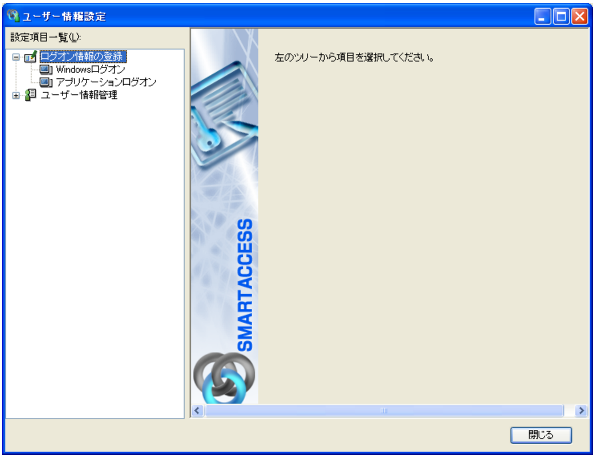
認証を要求するウィンドウが表示されます。

■ 例：指紋センサーをお使いの場合の認証要求ウィンドウ



2 認証情報を入力し、ログインします。

認証情報は利用する認証デバイスによって異なります。
「ユーザー情報設定」が起動します。



3 ログオン認証された利用者のユーザー情報が表示されます。

左側の、機能をツリー構造で表示している領域を「設定項目一覧」と呼び、右側には「設定項目一覧」から選択した機能の設定内容を表示します。
「設定項目一覧」には、導入されてない認証デバイスやインストールされていない連携ソフトウェアは表示されません。また、設定内容には「環境設定」で設定されている利用者固有の設定内容が表示されます。

POINT

- 「ユーザー情報設定」を終了するには、「閉じる」をクリックします。

6 セキュリティ環境の構築

セキュリティ環境の構築は、管理者が「環境設定」で行います。また、利用者固有の情報設定は利用者が「ユーザー情報設定」で行います。
SMARTACCESS によるセキュリティ環境の構築手順を例に、基本的な流れを説明します。

ここでは指紋認証を例にとり、コンピュータの起動時および Web サイトの接続時の認証を指紋認証に設定する手順を説明します。
スマートカードなどの認証デバイスをお使いになる場合も、同様の手順で設定します。
セキュリティ構築手順の基本的な流れは次のとおりです。

1 認証パターンの登録の確認（→ P.74）

2 アカウントの登録（→ P.77）

1. SMARTACCESS アカウントの登録
2. Windows ユーザーの登録
3. アカウント登録のための認証
   認証デバイスとしてセキュリティチップのみをお使いになる場合は、必要ありません。

3 Windows ログオンの設定（→ P.85）

必要に応じて行います。

4 アプリケーションログオンの設定

必要に応じて行います。

1. アプリケーションログオンを有効にする（→ P.87）
2. パスワード入力画面の登録（→ P.87）
3. アプリケーションログオン情報の登録（→ P.101）
   「アプリケーションログオン」を設定した場合、利用者が「ユーザー情報設定」でアプリケーションログオン情報の登録を行います。

認証パターンの登録の確認

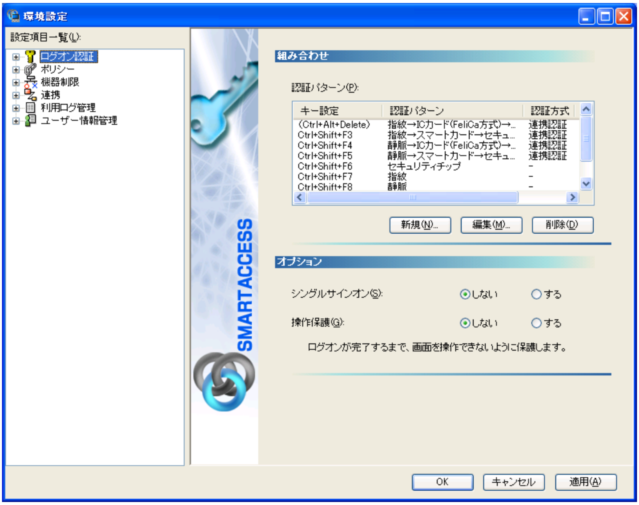
認証パターンには、ドライバがインストールされている認証デバイスが自動的に登録され、一覧で表示されます。

1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。

「環境設定」が起動します。

2 「設定項目一覧」から「ログオン認証」をクリックします。

3 **「認証パターン」の一覧にドライバをインストールした認証デバイスが表示されていることを確認します。**



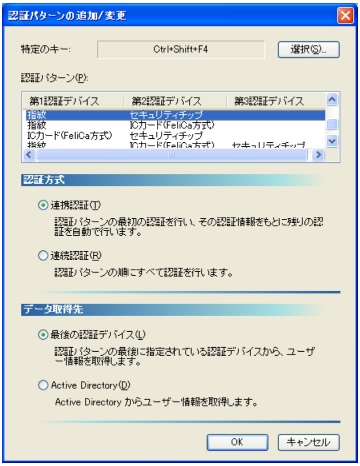
重要

- 「キー設定」は、「Windowsへようこそ」ウィンドウから認証ウィンドウに切り換える、または「ユーザー情報設定」の起動時に認証パターンを切り替えるときに使われるキーです。ご購入時の設定は「(Ctrl+Alt+Delete)」が登録されていますが、必要に応じて変更することができます。
  変更するには、「編集」をクリックし、「認証パターンの追加/変更」ウィンドウで行います。詳しくは、『リファレンスガイド』の「機能編」－「ログオン認証」－「ログオン認証の設定方法」をご覧ください。
- スマートカードホルダーが外された状態で SMARTACCESS をインストールすると、「認証パターン」に「スマートカード」が登録されません。その場合は、いったんSMARTACCESSをアンインストールしてからスマートカードホルダーを取り付けて再度SMARTACCESSをインストールしてください。
- 複数の認証デバイスをお使いになる場合は、「選択」をクリックして認証デバイスの組み合わせ、認証する順序および認証方式を登録します。詳しくは、『リファレンスガイド』の「機能編」－「ログオン認証」－「ログオン認証の設定方法」をご覧ください。

4 「キー設定」の（Ctrl+Alt+Delete）の隣に「指紋」が表示されていることを確認します。

「指紋」以外の認証パターンが表示されている場合には、次の手順で認証パターンを変更します。

1. （Ctrl+Alt+Delete）をクリックして選択し、「編集」をクリックします。
   「認証パターンの追加／変更」が起動します。



（画面は SMARTACCESS/Premium の例です）

2. 「第 1 認証デバイス」が「指紋」、「第 2 認証デバイス」が空白の組合せをクリックして「OK」をクリックします。

5 続けてアカウントの登録を行う場合は、「適用」をクリックします。

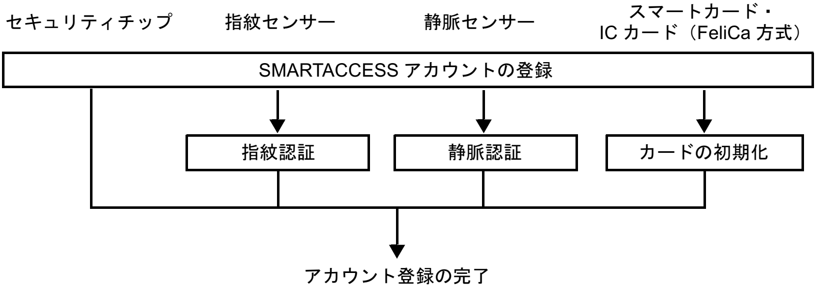
アカウントの登録を行う場合は、「アカウントの登録」（→ P.77）をご覧ください。

POINT

- 「環境設定」を終了するには、「OK」をクリックします。再起動を要求するウィンドウが表示された場合は、Windows を再起動して設定を有効にします。

アカウントの登録

SMARTACCESS を利用する管理者や利用者のアカウントは、「管理者ウィザード」で登録します。
お使いの認証デバイスによってアカウントの登録の手順は異なります。「管理者ウィザード」を利用したアカウントの登録手順は次のとおりです。



重要

- 「環境設定」の「ポリシー」でパスワードの複雑さなどが設定されている場合は、そのパスワード制限に準じます。
- スタンドアロンまたはワークグループ環境で利用しているコンピュータの場合、Windows アカウントは Administrators グループに所属している必要があります。
- ドメイン環境で利用しているコンピュータの場合、Windows アカウントは、ActiveDirectory（ドメインコントローラ）の Domain Admins グループに所属している必要があります。
- 指紋センサーをお使いの場合、「セキュリティ環境の構築」（→ P.74）後に利用者自身の指紋を登録する必要があります（→ P.94）。
- 静脈センサーをお使いの場合、「セキュリティ環境の構築」（→ P.74）後に利用者自身の静脈を登録する必要があります（→ P.94）。
- SMARTACCESS/Premium でバイオ認証装置連携をお使いの場合、SMARTACCESS アカウントの「アカウント名」と「パスワード」は、バイオ認証装置に登録されている「ユーザー名」と「パスワード」と同じ情報を登録します。

■管理者と利用者のアカウントの登録

ここでは、指紋センサーを使ったセキュリティ環境で、新規に管理者と利用者を順に登録する手順を説明します。

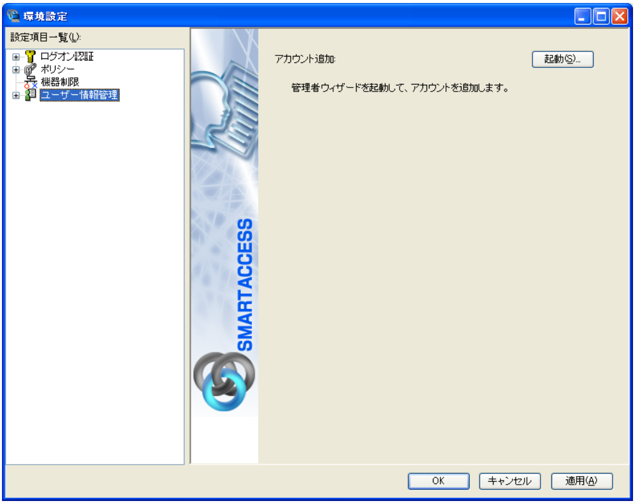
重要

- 指紋センサーをお使いで、指紋認証をローカルコンピュータで行う場合、アカウントの登録には認証が必要です。アカウントを登録するために、ご購入時の設定で「saadmin」アカウントを用意しています。

1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。

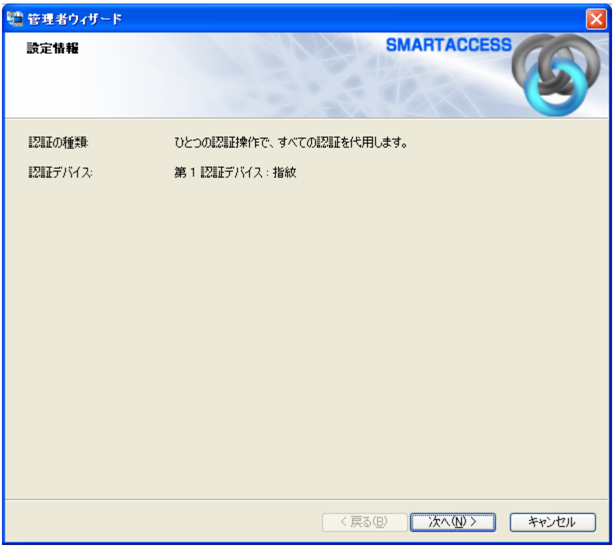
「環境設定」が起動します。

2 「設定項目一覧」から「ユーザー情報管理」をクリックします。



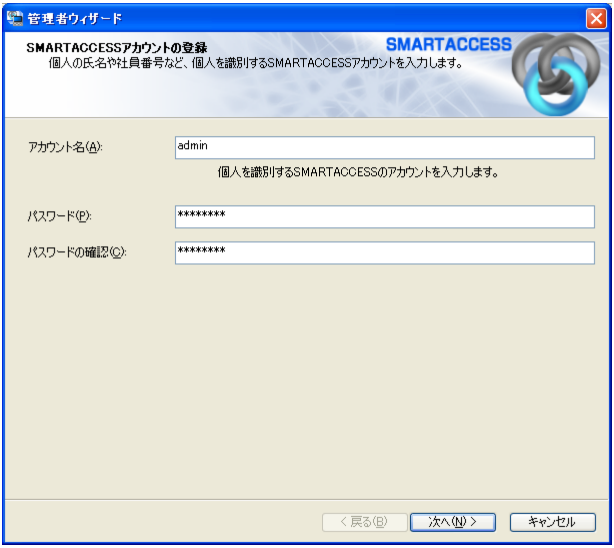
3 「アカウントの追加」から「起動」をクリックします。

「管理者ウィザード」ウィンドウが表示されます。



4 内容を確認し、「次へ」をクリックします。

「SMARTACCESS アカウントの登録」が表示されます。



5 SMARTACCESS で使用する管理者アカウントを登録します。

- **アカウント名**

  個人を識別するアカウントを入力します。
  - 認証デバイスに指紋または静脈が含まれる場合
    - 1 ～ 16 文字の半角英数字と記号 $()@_-.% で指定します。
    - バイオ認証装置を使用しない設定の場合、重複するユーザー名を使用することはできません。
    - バイオ認証装置連携をお使いの場合

      バイオ認証装置に登録されている「ユーザー名」と同じ情報を登録します。

      既に情報が設定されているアカウント名を入力すると登録情報を追加または上書きします。
  - 指紋および静脈が含まれない場合
    - 文字数や使用文字の制限はありません。
    - 重複するユーザー名を使用することができます。
- **パスワード**

  パスワードを入力します。

  ポリシーで複雑さの設定を行っている場合はその設定に従って指定します。

  複数のデバイスを使用する場合は、アカウント、パスワードは認証デバイスごとの条件をすべて満たすものを設定します。

  ここで入力したパスワードは、認証パターンに含まれているすべての認証デバイスのパスワードとして、同一のパスワードが設定されます。
  - 認証デバイスに指紋または静脈が含まれる場合

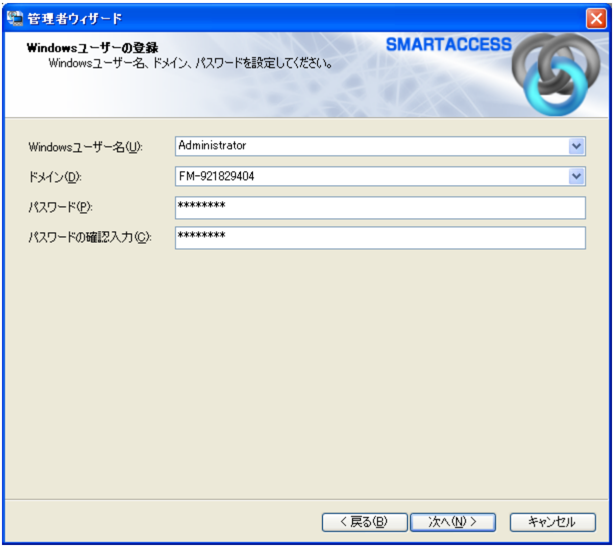
    バイオパスワードとして 8 ～ 32 文字の半角英数字と記号 $()@_-.% で指定します。

・バイオ認証装置連携をお使いの場合
バイオ認証装置に登録されている「パスワード」と同じ情報を登録します。
・認証デバイスにセキュリティチップが含まれる場合
ユーザーキーパスワードとして 6 ～ 256 文字の半角英数字と記号で指定します。
・認証デバイスに IC カード（FeliCa 方式）、およびスマートカードが含まれる場合
PIN として 1 ～ 16 文字の半角英数字と記号で指定します。

・パスワードの確認入力
「パスワード」で入力したのと同じ内容を入力します。

6 「次へ」をクリックします。

「Windows ユーザーの登録」が表示されます。



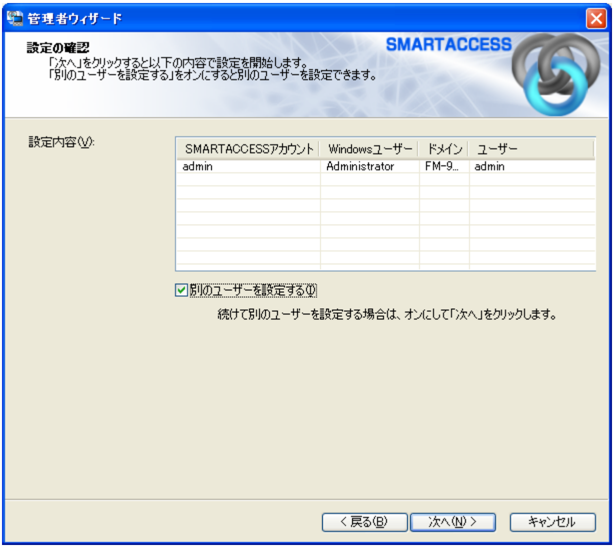
7 管理者用の Windows ユーザーを登録します。

「Windows ユーザー名」と「ドメイン」、「パスワード」、「パスワード入力確認」を入力し、「次へ」をクリックします。

重 要

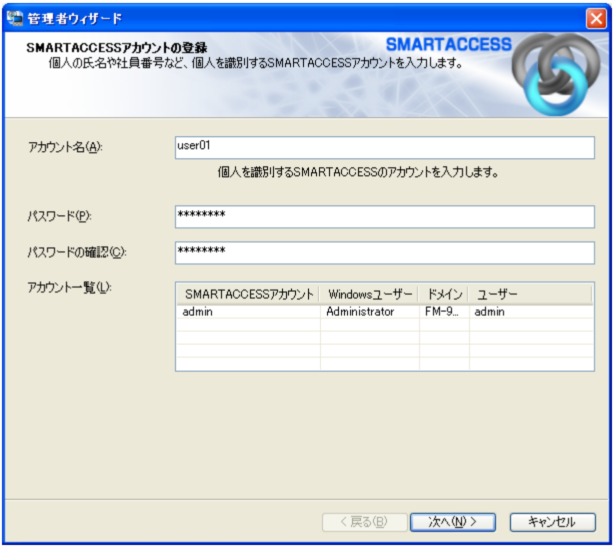
- 「Windows ユーザー名」、「パスワード」は、SMARTACCESS アカウントの「アカウント名」、「パスワード」と異なる情報で登録可能です。
- すでに Windows アカウントが登録されている場合、「Windows ユーザー名」の▼をクリックしてユーザー名を選択できます。
- ドメインに参加している場合は、「ドメイン」の▼をクリックしてドメインを選択できます。
- 「ドメイン」を選択してから、「Windows ユーザー名」の▼をクリックするとそのドメインのユーザーアカウントを選択できます。
- 「パスワード」には、Windows アカウントで登録されているパスワードを入力します。
- 「パスワード入力確認」には、「パスワード」と同じ情報を入力します。

「設定の確認」が表示されます。



8 **「別のユーザーを設定する」をチェックして「次へ」をクリックすると、続けて利用者のアカウントを登録できます。**

「SMARTACCESS アカウントの登録」が表示されます。
アカウントの登録を終了する場合は手順 12 に進みます。



9 **SMARTACCESS で使用する利用者アカウントを登録します。**
「アカウント名」と「パスワード」、「パスワード入力確認」を入力して、「次へ」をクリックします。

各入力項目の制約などについては、手順 5 をご覧ください。
「Windows ユーザーの登録」が表示されます。

10 **利用者用の Windows ユーザーを登録します。**

「Windows ユーザー名」と「ドメイン」、「パスワード」、「パスワード入力確認」を入力し、「次へ」をクリックします。
各入力項目の制約などについては、手順 7 をご覧ください。
「設定の確認」が表示されます。

11 **続けて別の利用者のアカウントを登録する場合は、「別のユーザーを設定する」をチェックして「次へ」をクリックします。**

「SMARTACCESS アカウントの登録」が表示されます。
アカウントの登録を終了する場合は手順 12 に進みます。

12 アカウントの登録を終了するには、「別のユーザーを設定する」のチェックを外して「次へ」をクリックします。

「指紋認証」ウィンドウが表示されます。

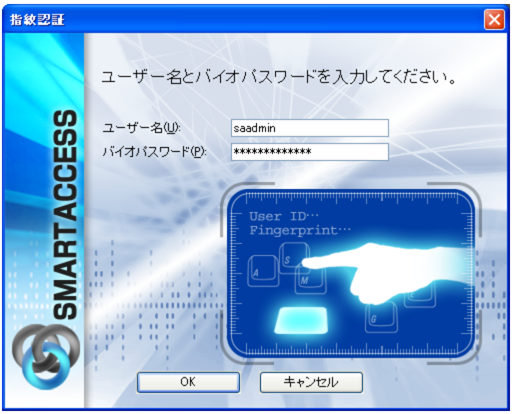


重要

- スマートカードおよび IC カード（FeliCa 方式）をお使いの場合、カードのセットを要求するウィンドウが表示されますので、リーダ／ライタにカードをセットします。また、スマートカードをお使いの場合、カードのセットを要求するウィンドウ表示後、管理者 PIN による認証ウィンドウが表示されますので「administrator」と入力して認証を行ってください。
  「完了」と表示されます。手順 15 に進んでください。
- セキュリティチップをお使いの場合は、「完了」と表示されます。手順 15 に進んでください。

13 指紋の登録を行っていないので、バイオパスワード認証に切り替えるために【F10】キーを押します。

「ユーザー名とバイオパスワードを入力してください。」と表示されます。

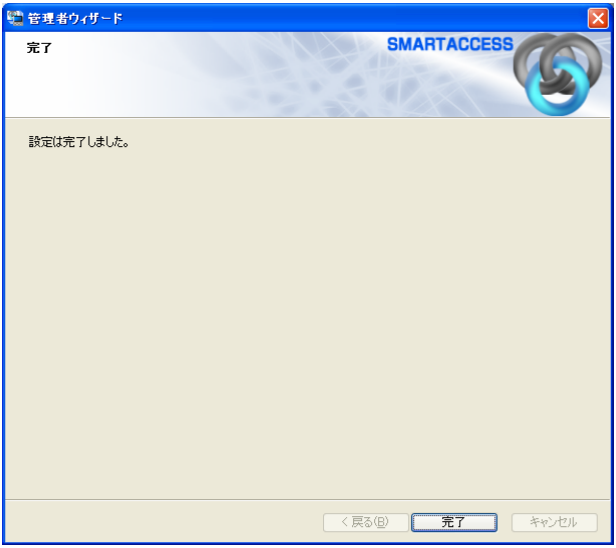


14 指紋認証をローカルコンピュータで行う場合は、「ユーザー名」に「saadmin」、「バイオパスワード」に「administrator」と入力し、「OK」をクリックします。

「完了」と表示されます。

■ 指紋認証をバイオ認証装置で行う場合

バイオ認証装置に登録されている「ユーザー名」と「パスワード」を入力し、「OK」をクリックします。

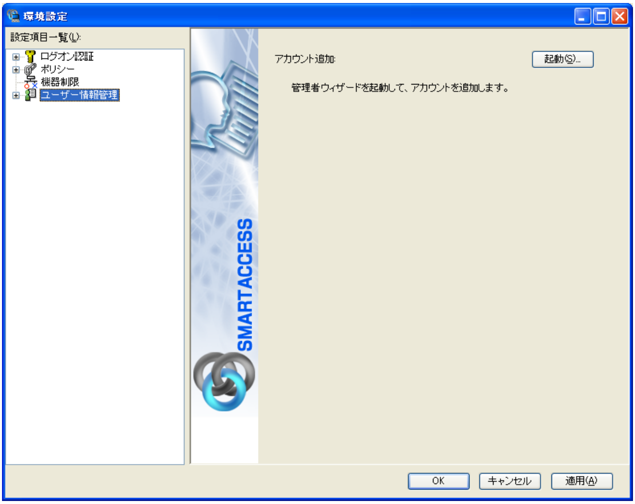


重要

- ユーザー名「saadmin」は、指紋認証をローカルコンピュータで行われる場合に利用する、ご購入時の指紋認証用の管理者アカウントです。
  管理者の登録完了後、ユーザー名「saadmin」を削除することをお勧めします。ユーザー名の削除については、『リファレンスガイド』の「ツール編」－「環境設定」－「ユーザー情報管理」－「指紋」をご覧ください。

15 「完了」をクリックします。

「環境設定」に戻ります。



16 続けて Windows ログオンの設定を行う場合は、「適用」をクリックします。

Windows ログオンの設定を行う場合は、「Windows ログオンの設定」（→ P.85）をご覧ください。

POINT

- 「環境設定」を終了するには、「OK」をクリックします。再起動を要求するウィンドウが表示された場合は、Windows を再起動して設定を有効にします。

Windows ログオンの設定

SMARTACCESS は Windows へのログオンを、認証デバイスを利用したログオンに置き換えることができます。
ここでは、Windows のログオン認証を、従来の Windows パスワードの認証から SMARTACCESS のデバイス認証に変更する手順を説明します。
Windows ログオンに関連する他の機能については『リファレンスガイド』の「機能編」－「Windows ログオン」をご覧ください。

■ Windows ログオンを有効にする

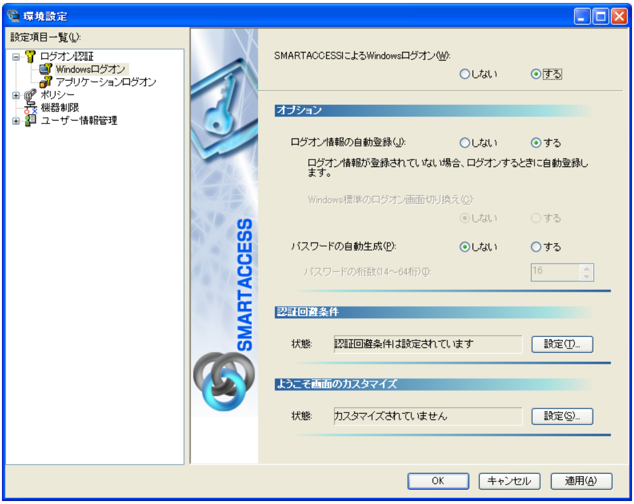
Windows ログオンを利用するには、「SMARTACCESS による Windows ログオン」を有効にします。

1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。

「環境設定」が起動します。

2 「設定項目一覧」から「ログオン認証」→「Windows ログオン」の順にクリックします。

3 「SMARTACCESSによるWindowsログオン」の「する」をクリックします。



4 続けてアプリケーションログオンの設定を行う場合は、「適用」をクリックします。

アプリケーションログオンの設定を行う場合は、アプリケーションログオンの有効化に進みます（→ P.86）

POINT

- 「環境設定」を終了するには、「OK」をクリックします。再起動を要求するウィンドウが表示された場合は、Windows を再起動して設定を有効にします。

アプリケーションログオンの設定

「アプリケーションログオン」は、アプリケーションの起動時や Web サイトへの接続時のパスワード認証を SMARTACCESS で認証する機能です。
アプリケーションログオンに関連する他の機能については『リファレンスガイド』の「機能編」－「アプリケーションログオン」をご覧ください。

重要

- 「環境設定」で「アプリケーションログオン」を設定した場合、利用者は「ユーザー情報設定」で「アプリケーションログオン情報」を登録することにより Web サイトへのアプリケーションログオンを行うことができます（→ P.101）。

■アプリケーションログオンを有効にする

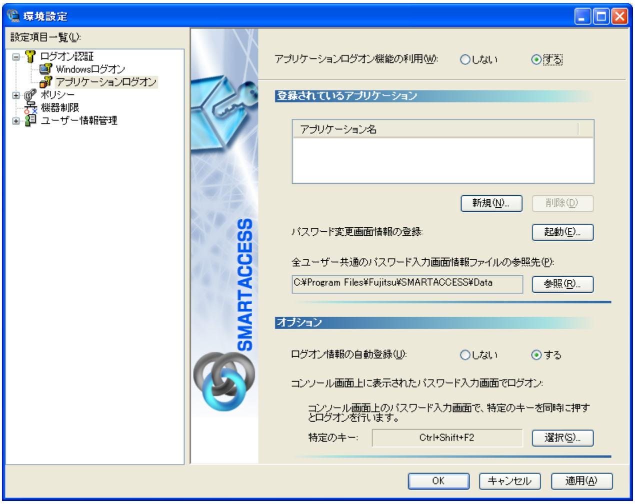
Internet Explorer で表示される Web サイトのパスワード認証を、SMARTACCESS のデバイスによる認証に置き換える手順を説明します。

1 **「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。**

「環境設定」が起動します。

2 **「設定項目一覧」から「ログオン認証」→「アプリケーションログオン」の順にクリックします。**

3 **「アプリケーションログオン機能の利用」の「する」をクリックします。**



4 **続けてパスワード入力画面の登録を行う場合は、「適用」をクリックします。**

パスワード入力画面の登録を行う場合は、「パスワード入力画面の登録」（→ P.87）をご覧ください。

POINT

- 「環境設定」を終了するには、「OK」をクリックします。再起動を要求するウィンドウが表示された場合は、Windows を再起動して設定を有効にします。

■パスワード入力画面の登録

アプリケーションログオン機能を使う Web サイトのパスワード入力画面を登録します。

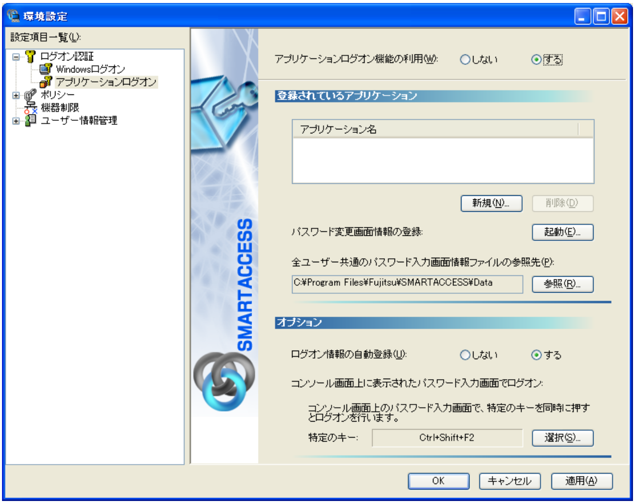
重要

- 「アプリケーションログオン」で関連付けする Web サイトは、認証サービスに対応している必要があります。

1 **「スタート」ボタン→「(すべての)プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。**

「環境設定」が起動します。

2 **「設定項目一覧」から「ログオン認証」→「アプリケーションログオン」の順にクリックします。**

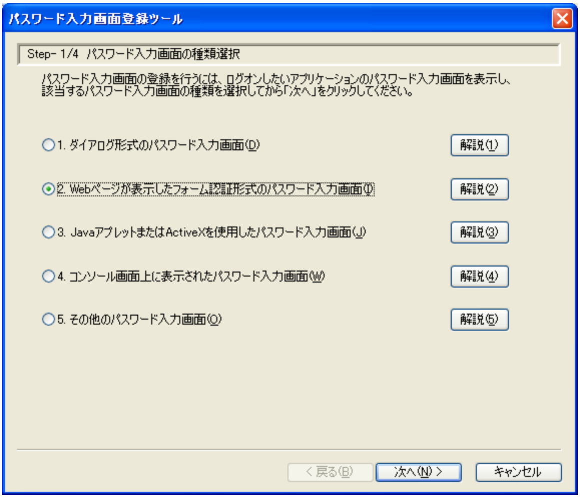


3 **「全ユーザー共通のパスワード入力画面情報ファイルの参照先」に参照先のフォルダが表示されていることを確認してから、「新規」をクリックします。**

POINT

- 「全ユーザー共通のパスワード入力画面情報ファイルの参照先」は SMARTACCESS の「パスワード入力画面」の設定情報を記述したファイルを格納するフォルダです。必要に応じて格納先を変更することができます。
- 参照先を変更する場合は、「参照」をクリックして参照先のフォルダを選択し、「適用」をクリックして設定を保存してください。
- 参照先に UNC(¥¥ で始まるパスの表記方式)を指定することにより、サーバー上のフォルダを指定できます。
  この場合、セキュリティ確保のため、フォルダの属性を利用者に対して読み取り専用とすることをお勧めします。
- 参照先に UNC を指定する場合、Windows へのログオン後に、エクスプローラを使って UNC で指定したサーバー上のフォルダ内を参照できるか確認してください。
  ユーザー名やパスワードが異なるためにエクスプローラから参照できない場合、パスワード入力画面情報ファイルを読み取ることができないため、アプリケーションログオン機能が正常に動作しません。

「パスワード入力画面登録ツール」が起動します。



「解説」をクリックすると、パスワード入力画面の種類の説明を表示します。
パスワード入力画面の種類については、『リファレンスガイド』の「機能編」－「アプリケーションログオン」－「パスワード入力画面の登録」－「パスワード入力画面のタイプ」をご覧ください。

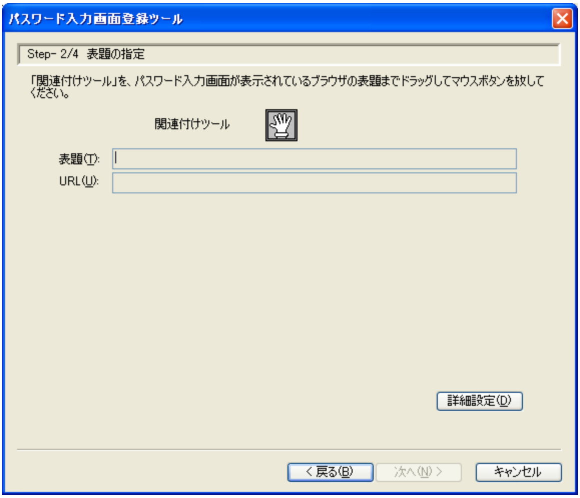
4 Internet Explorerを起動し、Webサイトに接続してパスワード入力画面を表示します。

重要

- 「Web ページが表示したフォーム認証形式のパスワード入力画面」をお使いになる場合は、ブラウザはInternet Explorerをお使いください。他のブラウザをお使いになる場合は、「JavaアプレットまたはActiveXを使用したパスワード入力画面」を選択します。詳しくは、『リファレンスガイド』の「ツール編」－「環境設定」－「アプリケーションログオン」－「パスワード入力画面登録ツール」をご覧ください。

5 「Web ページが表示したフォーム認証形式のパスワード入力画面」をクリックして、「次へ」をクリックします。

「Step-2/4 表題の指定」と表示されます。

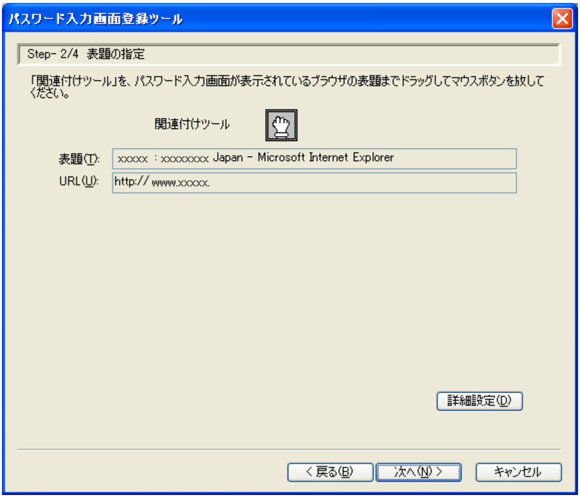


POINT

- 接続した Web サイトのパスワード入力画面に「パスワード入力画面登録ツール」ウィンドウが隠れている場合は、タスクバーなどで「パスワード入力画面登録ツール」ウィンドウをアクティブにします。

6 「関連付けツール」アイコン を Web サイトの表題にドラッグし、パスワード入力画面の表題を指定します。

「表題」「URL」にドラッグした Web サイトのパスワード入力画面のタイトルと URL が入力されます。



POINT

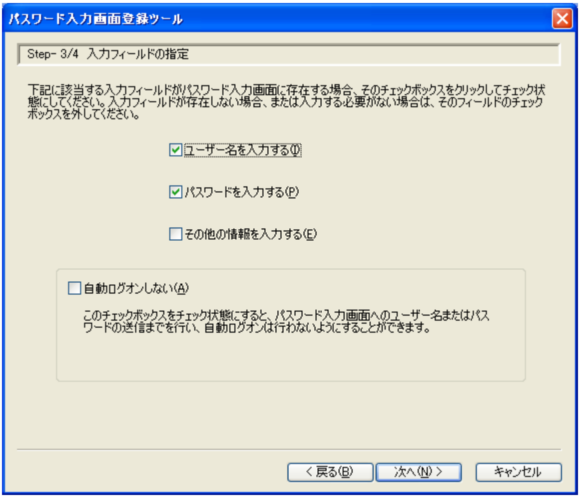
- 次の例のように「関連付けツール」を Web サイトのパスワード入力画面のタイトルバーにドラッグします。



「関連付けツール」は関連付けが設定できると、表示が から に変わります。

7 内容を確認して、「次へ」をクリックします。

「Step-3/4 入力フィールドの指定」と表示されます。

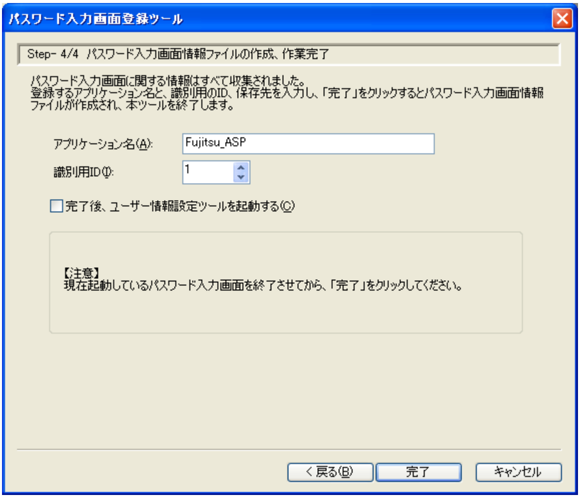


POINT

- Web サイトの入力フィールドがパスワードのみの場合は「パスワードを入力する」だけにチェックをしてください。

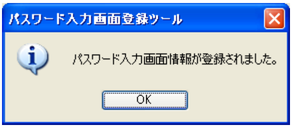
8 「ユーザー名を入力する」と「パスワードを入力する」にチェックが入っていることを確認して、「次へ」をクリックします。

「Step-4/4 パスワード入力画面情報ファイルの作成、作業完了」と表示されます。



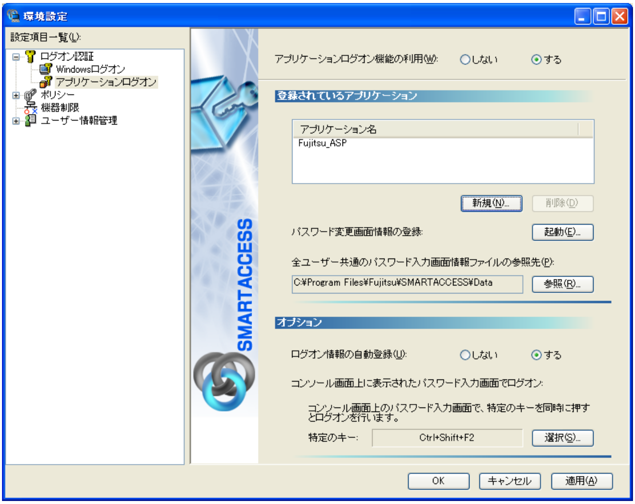
9 「アプリケーション名」を入力して、「完了」をクリックします。

「パスワード入力画面情報が登録されました。」という確認ウィンドウが表示されます。



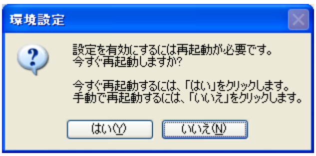
10 「OK」をクリックして、「環境設定」に戻ります。

登録したWebサイトを表示しているInternet Explorerのウィンドウを閉じてください。



11 「OK」をクリックして、「環境設定」を終了します。

再起動を要求するウィンドウが表示されます。



12 「はい」をクリックしてWindowsを再起動し、設定を有効にします。

重要

- Internet Explorer のクロススクリプティング問題への対策により、パスワード入力画面が frame タグを使用してほかの URL を参照している場合、正しくログオンできない場合があります。この場合、参照先の URL をインターネットオプションで「信頼済みサイト」として登録しておく必要があります。

7 利用者固有のセキュリティ情報の設定

管理者が「環境設定」で構築したセキュリティ環境に加えて、利用者がSMARTACCESS の運用開始時に利用者固有のセキュリティ情報を設定します。
ここでは、「セキュリティ環境の構築」（→ P.74）で構築したセキュリティ環境に、利用者のユーザー情報（指紋など）やパスワードを設定する手順を例に説明します。

1 認証用のユーザー情報の登録（→ P.94）
指紋センサー、および静脈センサーをお使いになる場合、設定が必要です。

2 アプリケーションログオン情報の登録（→ P.101）
必要に応じて行います。

3 パスワードの変更（→ P.104）
セキュリティ強化のため、必ずパスワードや PIN を変更してください。

認証用のユーザー情報の登録

指紋センサーおよび静脈センサーをお使いになる場合は、認証用の指紋や静脈の登録が必要です。指紋および静脈の登録は、「ユーザー情報設定」で行います。
ここでは、指紋の登録手順を例に説明します。
静脈の登録手順については、『リファレンスガイド』の「機能編」－「バイオ認証装置連携」－「バイオ認証装置連携の導入」をご覧ください。

1 コンピュータを起動します。
「Windows へようこそ」ウィンドウが表示されます。

2 【Ctrl】+【Alt】+【Delete】キーを押します。

「Windows へログオン」ウィンドウの認証画面が表示されます。



3 【F10】キーを押して、バイオパスワード認証ウィンドウに切り換えます。

「Windows へログオン」ウィンドウの「ユーザー名とバイオパスワードを入力する」が表示されます。



4 指紋を登録する利用者アカウントの「ユーザー名」「バイオパスワード」を入力して、「OK」をクリックします。

Windows が起動します。

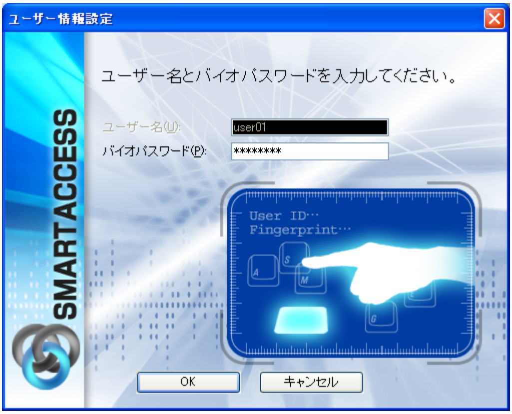
5 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「ユーザー情報設定」の順にクリックします。

「ユーザー情報設定」ウィンドウの認証画面が表示されます。



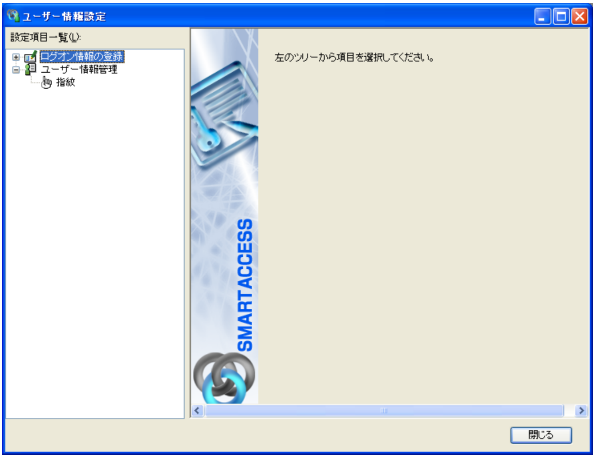
6 【F10】キーを押して、バイオパスワード認証ウィンドウに切り換えます。

「ユーザー情報設定」ウィンドウの「ユーザー名とバイオパスワードを入力する」が表示されます。



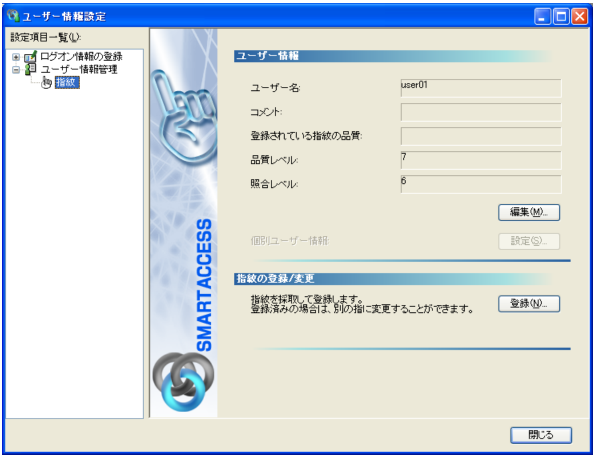
7 指紋を登録する利用者アカウントの「バイオパスワード」を入力して、「OK」をクリックします。

「ユーザー情報設定」ウィンドウが表示されます。



8 「設定項目一覧」から「ユーザー情報管理」→「指紋」の順にクリックします。

起動時に認証したアカウントの指紋情報が表示されます。



9 内容を確認して、「登録」をクリックします。

「ユーザー名を入力し、指をスライドさせてください。」が表示されます。



POINT

- 指紋登録のとき、【F10】キーを押さずに手順 10 のバイオパスワード認証ウィンドウが最初に表示されるように設定を変更することができます。
  「環境設定」の「ポリシー」→「指紋」にある「認証モード」で「指紋登録時にバイオパスワード認証を使用」を「する」と設定します。詳しくは『リファレンスガイド』の「ツール編」－「環境設定」－「ポリシー」－「指紋」をご覧ください。

10 【F10】キーを押して、バイオパスワード認証ウィンドウに切り換えます。

「ユーザー名とバイオパスワードを入力してください。」が表示されます。



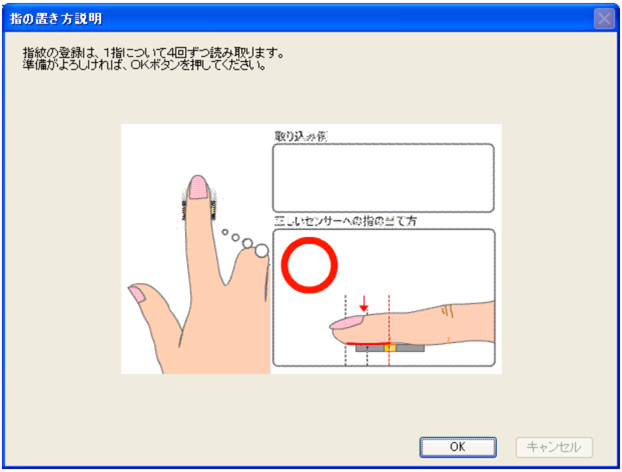
11 指紋を登録する利用者アカウントの「バイオパスワード」を入力して、「OK」をクリックします。

「指紋の登録／変更」ウィンドウが表示されます。



12 指紋を登録したい指をクリックして、「登録／変更」をクリックします。

「指の置き方説明」ウィンドウが表示されます。

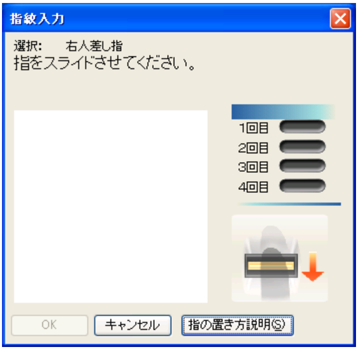


POINT

- 間違えて別の指をクリックした場合は、「キャンセル」をクリックして再度「登録／変更」をクリックし直します。

13 内容を確認して、「OK」をクリックします。

「指紋入力」ウィンドウが表示されます。



14 表示されるメッセージに従って、4 回指紋の読み取りを行い、「登録する指紋データを作成しました」と表示されたのを確認して「OK」をクリックします。

「指紋の登録／変更」ウィンドウが表示されます。

指紋の読み取り方については「認証デバイスについて」－「指紋センサー」－「取り扱い方」(→ P.24) をご覧ください。



15 **2 本目に登録する指をクリックし、手順 12 〜 14 の操作を行います。**

「指紋の登録 / 変更」ウィンドウが表示されます。



16 **登録した指にチェックマークが設定されていることを確認し、「OK」をクリックして、指紋情報を登録します。**

「ユーザー情報設定」ウィンドウに戻ります。

POINT

- 登録した指紋を取り消すには、登録した指をクリックして「削除」をクリックします。
- 「キャンセル」をクリックすると指紋の登録を中断して「ユーザー情報設定」ウィンドウに戻ります。

続けて「アプリケーションログオン情報」の登録を行う場合は、「アプリケーションログオン情報の登録」（→ P.101）をご覧ください。

POINT

- 「ユーザー情報設定」を終了するには、「閉じる」をクリックします。

アプリケーションログオン情報の登録

利用者のアプリケーションログオン情報の登録を行います。

重要

- 「アプリケーションログオン情報」を登録するには、「アプリケーションログオン」を利用する利用者アカウントで Windows にログオンする必要があります。
- 「アプリケーションログオン」を利用する利用者アカウントで、「ユーザー情報設定」を起動するときは利用者アカウントで認証します。
- 「アプリケーションログオン情報」を登録するには、事前に管理者が「環境設定」で「アプリケーションログオン」の設定を行っている必要があります。

1 **「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「ユーザー情報設定」の順にクリックします。**

「ユーザー情報設定」ウィンドウの認証画面が表示されます。

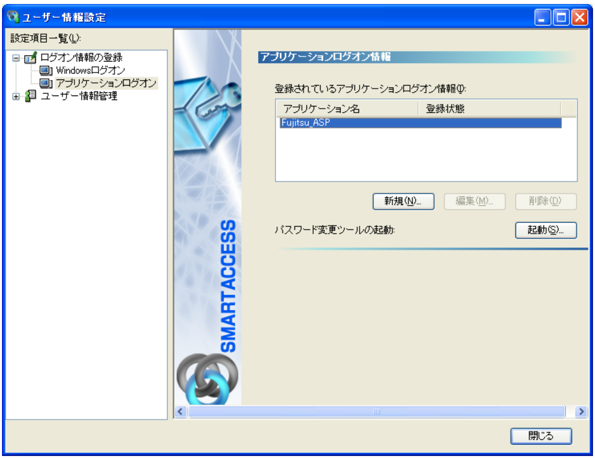


2 **ウィンドウのメッセージに従って指紋を入力します。**

認証されると「ユーザー情報設定」が起動します。

3 **「設定項目一覧」から「ログオン情報登録」→「アプリケーションログオン」の順にクリックします。**

「アプリケーションログオン情報」が表示されます。

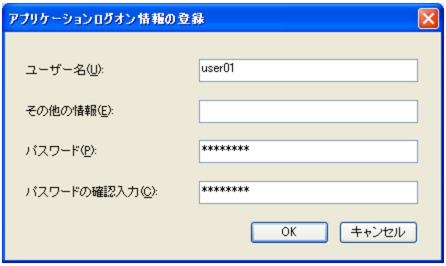


POINT

- 「登録されているアプリケーションログオン情報」には、管理者が「環境設定」で構築したアプリケーションログオン情報が一覧で表示されます。

4 登録するアプリケーション名をクリックして、「新規」をクリックします。

「アプリケーションログオン情報の登録」ウィンドウが表示されます。



5 「ユーザー名」「パスワード」「パスワードの確認入力」を入力して、「OK」をクリックします。

「ユーザー情報設定」ウィンドウに戻ります。

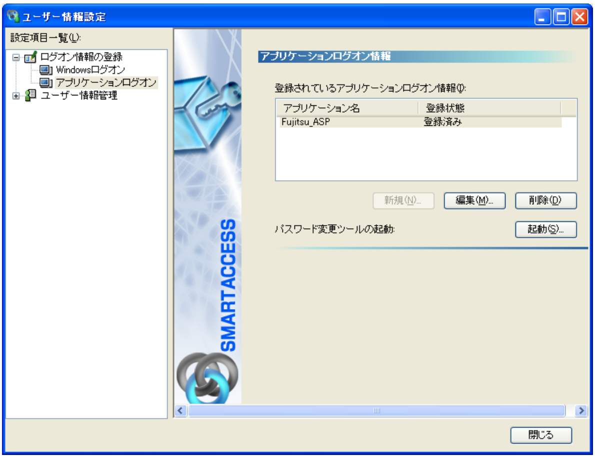
重要

- 「ユーザー名」「パスワード」には、Web サイトにログオンするときに必要なユーザー名とパスワードを入力します。

POINT

- 登録しているアプリケーションが「Web ページが表示したフォーム認証形式のパスワード入力画面」などの場合、「その他の情報」に入力する必要はありません。

登録が完了すると「登録されているアプリケーションログオン情報」のリストの「登録状態」の表記が「登録済み」と表示されます。



6 続けてパスワードの変更を行う場合は、「パスワードの変更」(→ P.104)をご覧ください。

POINT

- 「ユーザー情報設定」を終了するには、「閉じる」をクリックします。

パスワードの変更

利用者がパスワードやPINの変更をすることで、パスワードやPINを知っているのは利用者本人だけになります。セキュリティを強化するためにも、SMARTACCESS運用開始時に利用者がパスワードやPINを変更することをお勧めします。

アカウントには、「Windows アカウント」と認証デバイスで利用する「SMARTACCESS アカウント」があります。SMARTACCESS の運用を開始すると、ログオン時に入力するアカウント情報は、認証デバイスで利用する SMARTACCESS アカウントになります。
ここでは、指紋センサーで利用する SMARTACCESS アカウントのバイオパスワードの変更を説明します。

重要

- 利用者がパスワードを変更するには、利用者アカウントで Windows にログオンする必要があります。また、「ユーザー情報設定」を起動するときは利用者アカウントで認証します。

1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「ユーザー情報設定」の順にクリックします。

「ユーザー情報設定」ウィンドウの認証画面が表示されます。



2 ウィンドウのメッセージに従って指紋を入力します。

認証されると「ユーザー情報設定」が起動します。

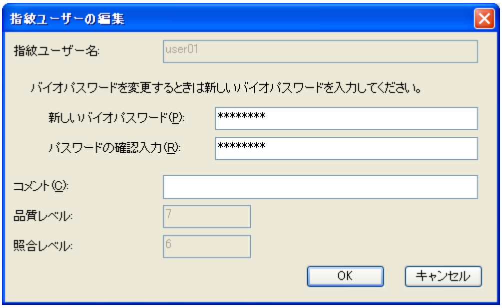
3 「設定項目一覧」から「ユーザー情報管理」→「指紋」の順にクリックします。

起動時に認証したアカウントの指紋情報が表示されます。



4 「編集」をクリックします。

「指紋ユーザーの編集」ウィンドウが表示されます。



5 「新しいバイオパスワード」「パスワードの確認入力」を入力し、「OK」をクリックします。

「ユーザー情報設定」ウィンドウに戻ります。

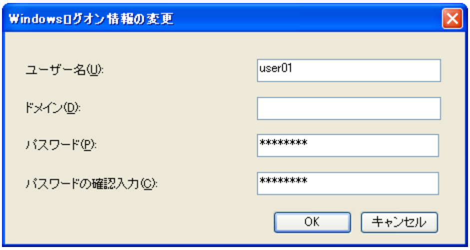
重要

- 指紋センサーおよび静脈センサーのバイオパスワード制限は次のとおりです。
  8 ～ 32 文字の半角英数字と記号 $()@_-.%
  指紋センサー、静脈センサー以外の認証デバイスのパスワード制限は次のとおりです。
  ・スマートカード、IC カード（FeliCa 方式）の場合
  1 ～ 16 文字の半角英数字と記号
  ・セキュリティチップの場合
  6 ～ 256 文字の半角英数字と記号
- 「ポリシー」で複雑さの設定を行っている場合は、設定されているパスワード制限に従って指定します。

6 「閉じる」をクリックして、「ユーザー情報設定」を終了します。

重要

- 利用者が Windows アカウントのパスワードの変更は、「ユーザー情報設定」で「ログオン情報登録」→「Windows ログオン」の「編集」をクリックして表示される、「Windows ログオン情報の変更」ウィンドウで行います。詳しくは、『リファレンスガイド』の「ツール編」－「ユーザー情報設定」－「ログオン情報の登録」－「Windows ログオン」をご覧ください。



8 SMARTACCESS の利用

管理者および利用者によるセキュリティ環境の構築が完了すると、利用者はSMARTACCESS の機能を利用することができます。

Windows ログオン

ここでは、指紋センサーを利用して Windows ログオンをする手順を説明します。

1 コンピュータを起動します。

「Windows へようこそ」ウィンドウが表示されます。

2 【Ctrl】+【Alt】+【Delete】キーを押します。

「Windows へログオン」ウィンドウの認証画面が表示されます。

重要

- 「認証パターン」を切り替える場合、現在表示されている認証画面が IC カード（FeliCa 方式）またはスマートカードで、カードがセットされている状態の場合は「認証パターン」を切り替えることができません。あらかじめカードを抜き取っておくか、認証画面で「キャンセル」ボタンをクリックして「Windows へようこそ」ウィンドウを表示させ、カードを抜き取ってから「認証パターン」を切り替えてください。

3 ウィンドウのメッセージに従って「ユーザー名」を入力して、指紋の読み取りを行います。

認証されると、Windows にログオンします。



重要

- 「ユーザー名」には、認証デバイスで利用する「SMARTACCESS アカウント」を入力します。

アプリケーションログオン

ここでは、Internet Explorer 経由で Web サイトに接続するとき、指紋センサーを利用して認証する手順を説明します。

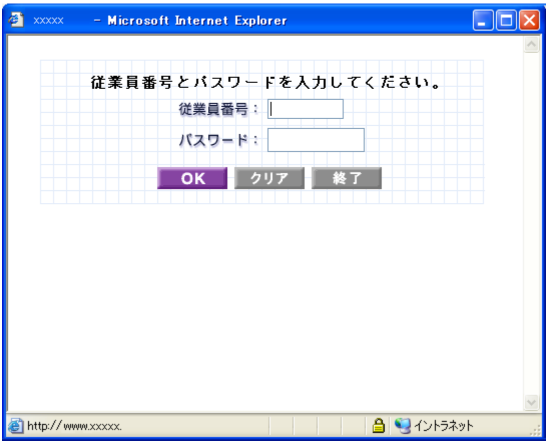
1 **Internet Explorer を起動して、Web サイトに接続します。**

「アプリケーションログオン」ウィンドウが表示されます。



2 **ウィンドウのメッセージに従って、指紋の読み取りを行います。**

指をスライドして読み取りを行うと、Web サイトの認証用ページが表示され、ユーザー名、パスワードなどが自動入力されて認証が行われます。



認証されると、目的の Web ページが表示されます。

9 アンインストール

SMARTACCESS のアンインストール

SMARTACCESS のアンインストールは、次の手順で行います。

重要

- アンインストールをするには、SMARTACCESS をインストールした管理者権限をもつアカウントでログオンしている必要があります。
- 暗号化したファイルやメールなどがある場合は、暗号化を解除してからアンインストールを行ってください。
- パスワードの自動生成を行っている場合は、いったん「パスワードの自動生成」を「しない」にした後、「パスワードの変更」（→ P.104）の手順で任意のパスワードに変更してからアンインストールを行ってください。
  パスワードの自動生成の解除については『リファレンスガイド』の「機能編」－「Windows ログオン」－「パスワードの自動生成」をご覧ください。
- SMARTACCESS/Premium でFENCE-GやSystemwalkerとの連携機能をお使いの場合、連携するソフトウェア側で連携機能を行わない設定をしてから SMARTACCESS のアンインストールを行ってください。
- 再起動の要求があった場合は、必ず再起動を行ってください。

1 「スタート」ボタン→「コントロールパネル」の順にクリックします。

「コントロールパネル」ウィンドウが表示されます。

2 次の操作をします。

■ Windows XP の場合

「プログラムの追加と削除」をクリックします。

■ Windows 2000 の場合

「アプリケーションの追加と削除」をダブルクリックします。

3 「SMARTACCESS」をクリックし、「削除」をクリックします。

この後は、メッセージに従って操作します。

POINT

- SMARTACCESS/PremiumV1.1L21またはSMARTACCESS/BasicV1.1L21がインストール済みの環境で、SMARTACCESS/PremiumV1.1L21またはSMARTACCESS/BasicV1.1L21の「setup.exe」を実行しても、アンインストールが開始されます。
- 認証デバイスとしてセキュリティチップを使用している環境で、SMARTACCESS をアンインストール後に、再びセキュリティチップを使用して SMARTACCESS をインストールする場合、SMARTACCESS のアンインストール後に必ず Security Platform（Infineon TPM ProfessionalPackage）をアンインストールし、BIOS セットアップでセキュリティチップの鍵を消去する必要があります。
  Security Platform（Infineon TPM ProfessionalPackage）のアンインストールについては、「認証デバイスのアンインストール」（→ P.110）、およびセキュリティチップの「Readme.txt」（→

P.56）をご覧ください。
またセキュリティチップの鍵の消去については、コンピュータ本体の『製品ガイド』の「BIOS」ー「認証デバイスのセキュリティ機能を使う」をご覧ください。
なおセキュリティチップの鍵を消去すると、それまで使用していた鍵や証明書が使用できなくなります。セキュリティチップで管理されている鍵や証明書の情報を引き続きお使いになるには、SMARTACCESS をアンインストールする前にバックアップし、再インストール後にリストアを行なう必要があります。
バックアップとリストアの手順については、『リファレンスガイド』の「ツール編」ー「オプションツール」ー「バックアップツール」をご覧ください。

認証デバイスのアンインストール

認証デバイスのドライバのアンインストールは、「コントロールパネル」の「プログラムの追加と削除（Windows2000 の場合は、アプリケーションの追加と削除)」で行います。詳しくは、それぞれの認証デバイスの「Readme.txt」（→ P.56）をご覧ください。

■アンインストール時の注意事項

・ 認証デバイスのドライバをアンインストールする場合は、必ず SMARTACCESS をアンインストールしてからドライバのアンインストールを行ってください。
認証デバイスのドライバをアンインストールした状態で、SMARTACCESS によるログオンを行うと、Windows が正常に起動しなくなります。
・ 複数の認証デバイスをお使いの場合に、一部の認証デバイスのドライバをアンインストールするときは、必ず SMARTACCESS で「認証デバイスの削除」を行ってからドライバのアンインストールを行ってください。
「認証デバイスの削除」については、「認証デバイスの追加」（→ P.65）をご覧ください。
・ 認証デバイスのドライバをアンインストールするには、管理者権限で Windows にログオンする必要があります。
・ 再起動の要求があった場合は、必ず再起動を行ってください。

5

第 5 章

運用例

SMARTACCESS では、さまざまな認証デバイスやセキュリティ機能によって、安全なセキュリティ環境を構築できます。この章では、代表的な認証デバイスを利用するセキュリティ環境の事例を説明しています。

1 セキュリティチップで暗号化ファイルの鍵を保護する

セキュリティチップをお使いになると、電子メールや Windows 暗号化ファイルシステム（EFS）で利用される秘密鍵を保護することができます。

ここでは、セキュリティチップを利用するセキュリティ環境と Windows 暗号化ファイルシステム（EFS）の秘密鍵を保護する設定と利用について説明します。

重要

- Windows 暗号化ファイルシステム（EFS）は、Windows XP Professional および Windows 2000 でサポートされます。Windows XP Home Edition は、暗号化ファイルシステム（EFS）をサポートしておりません。
  Windows 暗号化ファイルシステム（EFS）をお使いになる場合は、ハードディスクのファイルシステムは NTFS でフォーマットする必要があります。
- Windows 暗号化ファイルシステム（EFS）を使ってファイルを暗号化する場合は、ファイルまたはフォルダのプロパティで設定します。ハードディスク全体またはボリューム全体を暗号化することはできません。
- 次のようなフォルダは暗号化しないでください。セキュリティチップが利用できなくなったり、コンピュータが起動できなくなったりする場合があります。
  ・Windows の起動に必要なファイルのあるフォルダ（C:¥Windows など）
  ・ユーザー情報の入ったフォルダ（C:¥Document and Settings¥ ＜ユーザー名＞など）
  ・ソフトウェアがインストールされているフォルダ（C:¥Program Files など）
- セキュリティチップのバックアップファイルを保存したフォルダは暗号化しないでください。セキュリティチップが利用できなくなる場合があります。

Windows 暗号化ファイルシステム（EFS）を有効にする

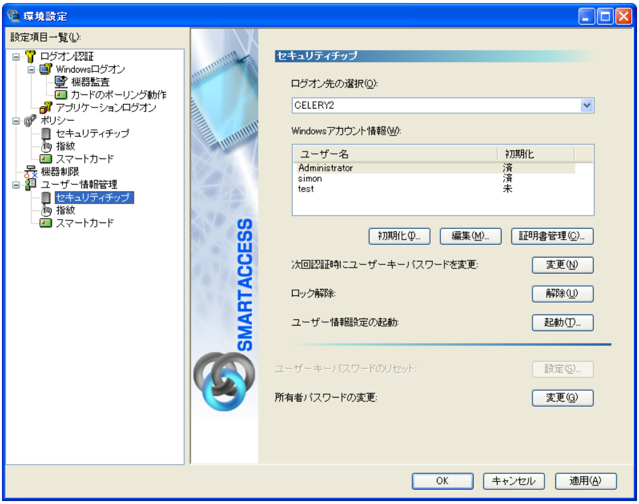
セキュリティチップで Windows 暗号化ファイルシステム（EFS）の秘密鍵を保護するには、管理者が利用者ごとに「環境設定」の「ユーザー情報管理」で設定します。
ここでは、セキュリティチップによる Windows 暗号化ファイルシステム（EFS）で必要となる証明書は新規に作成します。

1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。

「環境設定」が起動します。

2 「設定項目一覧」から「ユーザー情報管理」→「セキュリティチップ」の順にクリックします。

セキュリティチップの「ユーザー情報管理」の詳細が表示されます。



3 「Windowsアカウント情報」からWindows暗号化ファイルシステム(EFS)を利用する利用者の「ユーザー名」をクリックし、「初期化」をクリックします。

「Windows アカウント情報」の「初期化」が「未」の場合、「ユーザーの初期化」ウィンドウが表示されます。



認証パターンにセキュリティチップが含まれている場合は、管理者ウィザードの実行時にユーザーの初期化が完了しているため、「ユーザー初期化ウィザード」が起動します。手順 6 に進んでください。



重要

- 「環境設定」を起動している管理者以外の利用者の「ユーザー名」を選択すると、「セキュリティチップ」ウィンドウが表示されます。初期化する利用者の Windows パスワードを入力してください。

4 **「パスワード」および「パスワードの確認入力」にセキュリティチップで使用するユーザーキーパスワードを入力して、「OK」をクリックします。**

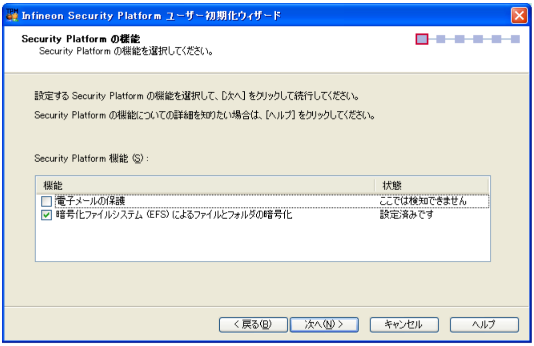
5 **もう一度「初期化」をクリックします。**

「ユーザー初期化ウィザード」が起動します。



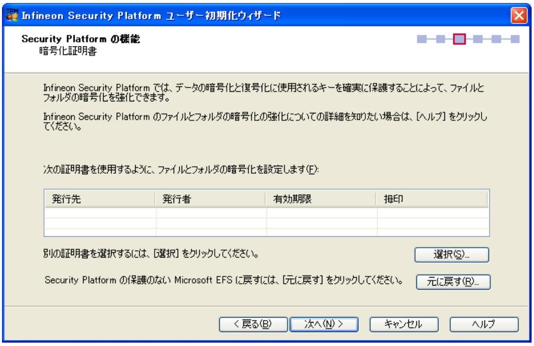
6 「次へ」をクリックします。

「Security Platform の機能－ Security Platform の機能を選択してください」と表示されます。



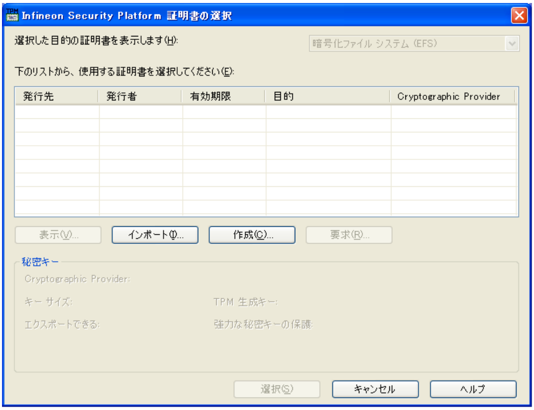
7 「暗号化ファイルシステム（EFS）によるファイルとフォルダの暗号化」をオンにし、「次へ」をクリックします。

「Security Platform の機能－暗号化証明書」と表示されます。



8 別の証明書を選択するには、「選択」をクリックします。

「証明書の選択」ウィンドウが表示されます。



重要

- セキュリティチュップで Windows 暗号化ファイルシステム（EFS）をお使いになるには証明書が必要です。一覧に表示されている証明書を利用する場合は、証明書を選択して「次へ」をクリックします。

9 新規に証明書を作成するために、「作成」をクリックします。

「ユーザー認証」ウィンドウが表示されます。



10 「基本ユーザー　パスワード」に利用者のユーザーキーパスワードを入力して、「OK」をクリックします。

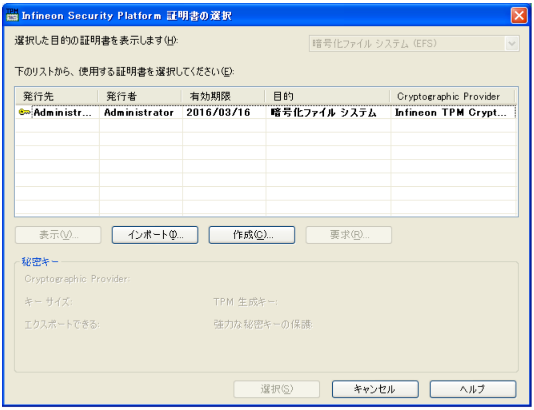
パスワード確認入力をするための「ユーザー認証」ウィンドウが表示されます。

重要

- 作成済みの証明書をお使いになる場合は、一覧から証明書を選択して「選択」をクリックします。

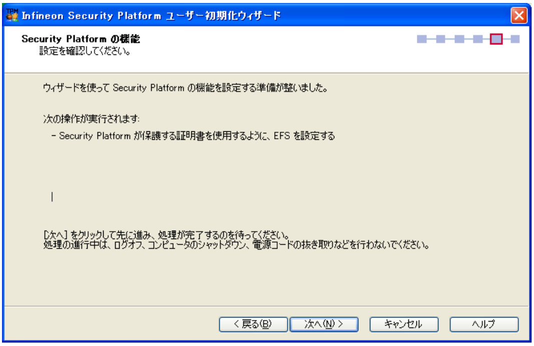
11 もう一度ユーザーキーパスワードを入力して、「OK」をクリックします。

「証明書の選択」ウィンドウに戻り、作成された証明書がリストに追加されます。



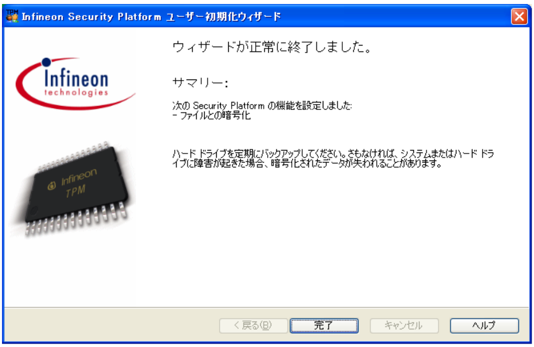
12 「次へ」をクリックします。

「Security Platform の機能－設定を確認してください」と表示されます。



13 「次へ」をクリックします。

「ウィザードが正常に終了しました。」と表示されます。



14 **「完了」をクリックします。**

15 **「環境設定」の「OK」をクリックします。**

続けて他の利用者の設定を行う場合は、「適用」をクリックし、手順 3 〜 13 を繰り返します。

16 **コンピュータを再起動します。**

Windows を再起動することで設定を有効にします。

Windows 暗号化ファイルシステム（EFS）の利用

Windows 暗号化ファイルシステム（EFS）は、通常の環境と同じように設定して利用することができます。ここでは、セキュリティチップを利用して Windows ログオンし、フォルダに Windows 暗号化ファイルシステム（EFS）の設定をするまでを説明します。
Windows 暗号化ファイルシステム（EFS）については、Windows のヘルプをご覧ください。

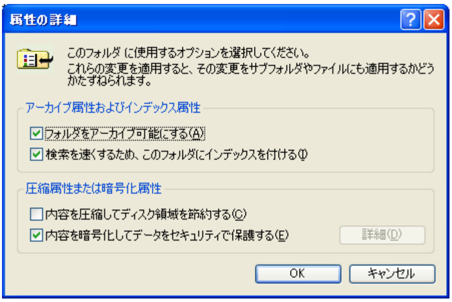
■ Windows 暗号化ファイルシステム（EFS）の設定

1 **Windows にログオン後、暗号化設定をするフォルダを右クリックして、「プロパティ」をクリックします。**

フォルダのプロパティのウィンドウが表示されます。

2 **「全般」タブの「詳細設定」をクリックします。**

「属性の詳細」ウィンドウが表示されます。



3 **「内容を暗号化してデータをセキュリティで保護する」をチェックし、「OK」をクリックします。**

ファイルまたはフォルダのプロパティのウィンドウに戻ります。

POINT

- 「内容を圧縮してディスク領域を節約する」を併用して設定することはできません。詳しくは、Windows のヘルプをご覧ください。

4 「OK」をクリックします。

「属性の変更の確認」ウィンドウが表示されます。

重要

- ファイルの場合は、「暗号化に関する警告」ウィンドウが表示されます。暗号化する対象を選択して、「OK」をクリックします。

5 暗号化する対象を選択して、「OK」をクリックします。

POINT

- Windows 暗号化ファイルシステム（EFS）を設定したファイルまたはフォルダに他の利用者がアクセスしようとすると、アクセス拒否するメッセージが表示されます。セキュリティチップによる Windows 暗号化ファイルシステム（EFS）を設定したファイルの秘密鍵はセキュリティチップで管理されます。セキュリティチップで管理された秘密鍵を外に持ち出すことはできないので、機密文書などを安全に保護することができます。

2 スマートカードの抜き取りによるコンピュータのロック

「カードのポーリング動作」機能をお使いになると、Windows にログオンするときにユーザー名やパスワードを入力する代わりにスマートカードをリーダ／ライタにセットすることでログオンできます。

スマートカードをお使いになることにより、パスワードの漏えいの危険がなくなり、コンピュータの不正利用やなりすましを防ぐことができます。また離席時にリーダ／ライタからスマートカードを抜き取るだけでコンピュータをロックすることができます。コンピュータのロックを解除するには、再度リーダ／ライタにスマートカードをセットします。

カードのポーリング動作

ここでは、スマートカードをリーダ／ライタから取り出したときにコンピュータをロックする設定を説明します。
「カードのポーリング動作」に関連する他の機能については『リファレンスガイド』の「機能編」－「Windows ログオン」－「カードのポーリング動作」をご覧ください。

重要

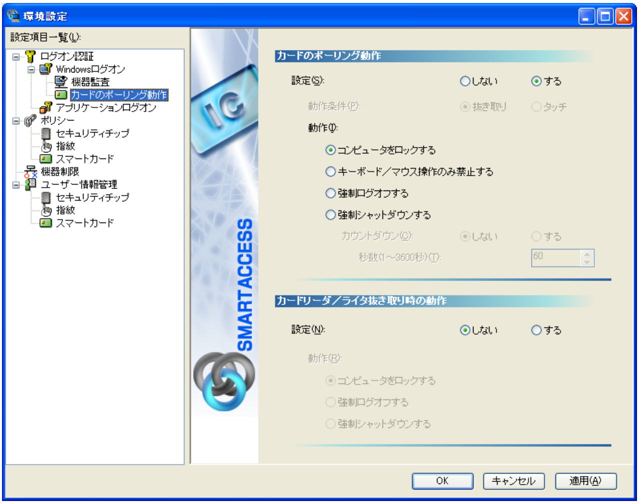
- あらかじめ認証パターンの組合せにスマートカードを設定し、「SMARTACCESS による Windows ログオン」を「する」に設定してください。

1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。

「環境設定」が起動します。

2 **「設定項目一覧」から「ログオン認証」→「Windows ログオン」→「カードのポーリング動作」をクリックします。**

「カードのポーリング動作」の詳細が表示されます。



3 **「カードのポーリング動作」－「設定」の「する」をクリックします。**

4 **「動作」の「コンピュータをロックする」をクリックし、「OK」をクリックします。**

重要

- 「カードのポーリング動作」を「強制ログオフする」または「強制シャットダウンする」に設定している場合は、Windows のアクティブデスクトップ機能を利用しないでください。

スマートカードの利用

カードのポーリング動作を設定すると、スマートカードを利用して Windows ログオンした後は、スマートカードを抜き取るだけでコンピュータをロックすることができます。
コンピュータのロックを解除する場合は、【Ctrl】+【Alt】+【Delete】キーを押した後、スマートカードをセットして PIN を入力します。

3 BIOS 指紋認証による Windows ログオン

BIOS 指紋認証を利用すると、コンピュータの起動時に BIOS に登録されている指紋を使って認証します。またシングルサインオンを有効にすると、コンピュータの起動時の指紋認証のみで Windows を起動することもできます。
BIOS 指紋認証は BIOS 指紋認証機能に対応しているコンピュータのみでお使いになれます。

ここでは、「Windows ログオンとのシングルサインオン」、「BIOS 指紋ユーザーの新規登録」、および「BIOS パスワードの有効化」の設定と利用について説明します。

BIOS 指紋認証の設定

BIOS 指紋認証の設定手順は次の手順で行います。

1 **「SMARTACCESS による Windows ログオン」を「する」に設定する（→ P.85）**
あらかじめ「認証パターン」の組合せに「指紋」を設定してから、「SMARTACCESS による Windows ログオン」を「する」に設定してください。

2 **BIOS シングルサインオンを有効にする（→ P.122）**

3 **BIOS 指紋ユーザーの登録（→ P.123）**

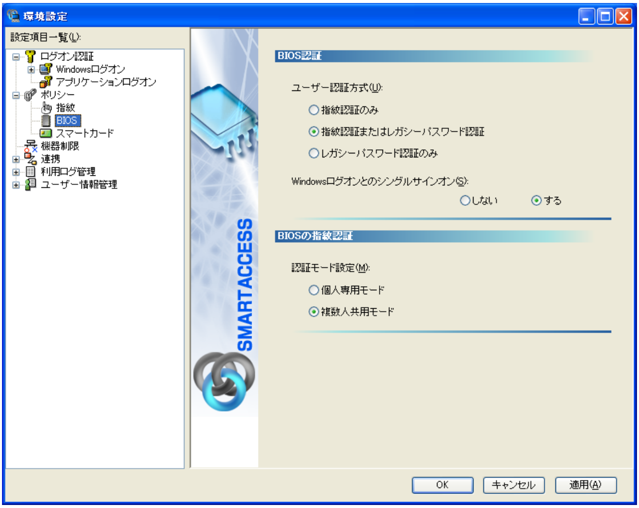
4 **BIOS パスワードを有効にする（→ P.124）**

■ BIOS シングルサインオンを有効にする

1 **「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。**
「環境設定」が起動します。

2 **「設定項目一覧」から「ポリシー」→「BIOS」をクリックします。**
「BIOS 認証」の詳細が表示されます。

3 **「Windowsログオンとのシングルサインオン」の「する」をクリックします。**



重要

- ご購入時の「ユーザー認証方式」は「指紋認証またはレガシーパスワード認証」となっています。「ユーザー認証方式」が「指紋認証のみ」の場合、登録した指紋の品質が悪い場合や指にけがをしたときに、コンピュータにログオンできなくなることがありますのでご注意ください。
- 指紋で認証して BIOS セットアップを起動すると、BIOS セットアップの「管理者」ではなく「ユーザー」となります。BIOS セットアップの「管理者」として認証するためには、指紋ではなくパスワードによる認証を行う必要があります。
  「ユーザー認証方式」を「指紋認証のみ」に設定している場合に、管理者として BIOS セットアップを起動するためには、いったん「ユーザー認証方式」を「指紋認証またはレガシーパスワード認証」に変更して再起動し、BIOS セットアップでの認証はパスワードで行ってください。

■BIOS 指紋ユーザーの登録

重要

- BIOS に指紋を登録するには、あらかじめ指紋のユーザーを登録し、さらに指紋を登録しておく必要があります。指紋を登録していないユーザーを BIOS に登録することはできません。

1 **「スタート」ボタン→「(すべての)プログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。**

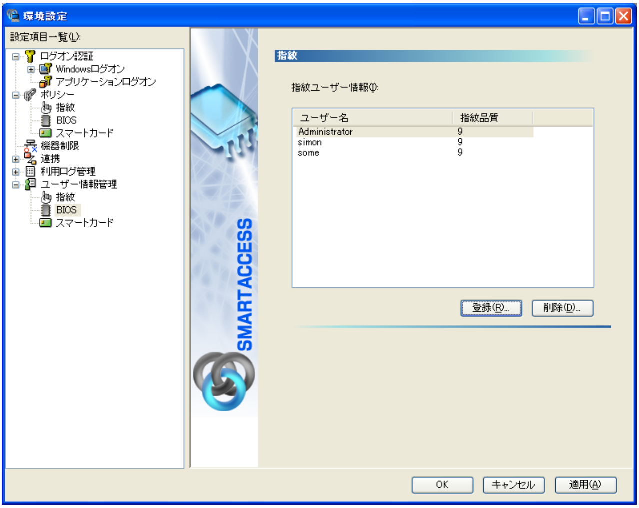
「環境設定」が起動します。

2 **「ユーザー情報管理」→「BIOS」の順にクリックします。**

指紋認証画面が表示されます。

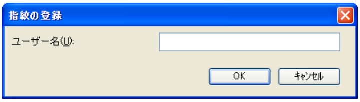
3 指紋を入力して認証を行います。

「指紋ユーザー情報」が表示されます。



4 「指紋ユーザー情報」の「登録」をクリックします。

「指紋の登録」ウィンドウが表示されます。



5 「ユーザー名」に指紋でログオンする SMARTACCESS アカウントを入力します。

重要

- ユーザー名は大文字小文字を区別します。BIOSに登録するときに入力するユーザー名は、指紋ユーザー名と一致するように入力してください。

6 登録の確認後、「環境設定」で「OK」をクリックします。

■BIOS パスワードを有効にする

コンピュータを再起動し、BIOS セットアップで起動時のパスワードを設定し、BIOS セットアップの起動時にパスワードの認証が必要となるようにします。
BIOS セットアップの起動と設定は、お使いのコンピュータによって異なります。詳しくは、コンピュータ本体の『製品ガイド』の「BIOS」をご覧ください。

BIOS 指紋を利用してログオンする

BIOS 指紋認証を利用して、Windows を起動します。

1 コンピュータを起動します。

指紋認証画面が表示されます。

2 認証タイプで「指紋認証」を選択し、指紋の読み取りを行います。



重要

- BIOS 指紋認証では指紋の情報をBIOS 内に格納しています。BIOS 内に格納されている情報を削除する場合は「ユーザー情報管理」→「BIOS」から、指紋ユーザー情報を削除する必要があります。

POINT

- Windows ログオン時には「Windows へようこそ」の画面が表示されます。

Memo

6

第 6 章

ネットワーク運用

ネットワークを利用して SMARTACCESS のセキュリティ環境を集中管理することができます。
この章では、「Active Directory 連携」と「バイオ認証装置連携」の導入を説明しています。
なお、ネットワーク運用は SMARTACCESS/Premium でお使いになれる機能です。

1 Active Directory 連携

「Active Directory連携」をWindowsドメイン環境に導入することで、SMARTACCESS設定情報をActive Directoryサーバーで集中管理することができます。これによりドメイン管理者の負担を軽減し、SMARTACCESSによるセキュリティ環境をドメイン内で標準化して管理することができます。

「Active Directory 連携」には、次のツールがあります。

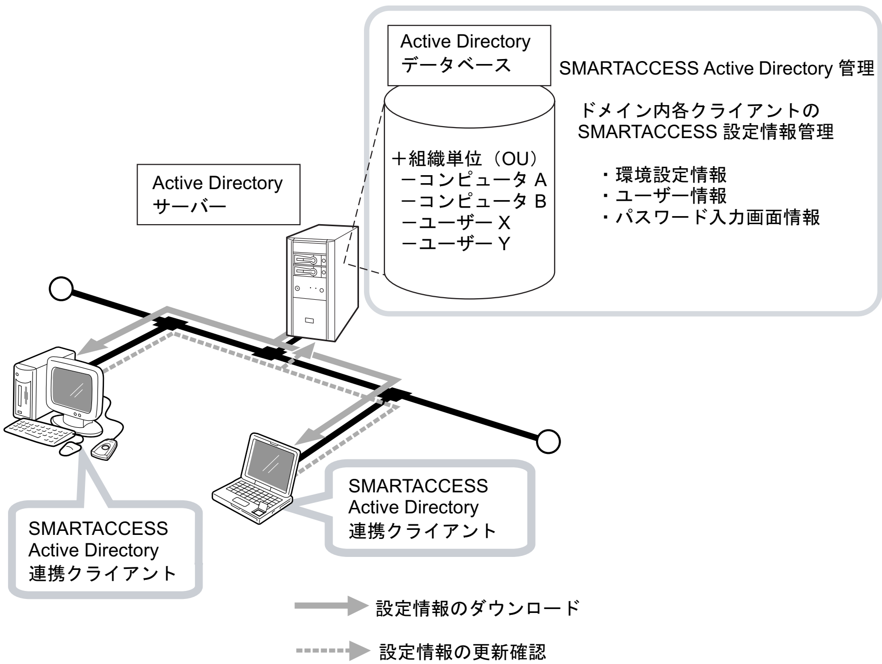
■ SMARTACCESS Active Directory 管理

SMARTACCESS Active Directory 管理（以下、Active Directory 管理）は、個々のコンピュータ上にある SMARTACCESS のセキュリティ環境を集中管理します。
「Active Directory 管理」が管理できる情報は次のとおりです。

- 環境設定情報
- ユーザー情報（Windows ログオン情報やアプリケーションログオン情報など）
- パスワード入力画面情報

■ SMARTACCESS Active Directory 連携クライアント

SMARTACCESS Active Directory 連携クライアント（以降、Active Directory 連携クライアント）は、設定情報の適用が必要かどうかを定期的に確認し、適用が必要な場合は「SMARTACCESS 更新確認」ウィンドウを表示してセキュリティ環境を新しい設定に適用させることができます。



Active Directory 連携の導入準備

Active Directory 連携を導入するには、次の条件を満たしている必要があります。

■システムの必要条件

項目	Active Directory 管理	Active Directory 連携クライアント
ハードディスク	70MByte 以上の空き容量	50MByte 以上の空き容量
OS	Windows Server 2003 Windows 2000 Server	Windows XP Professional Windows XP Tablet PC Edition 2005 Windows 2000 Professional
Windows ドメイン	Active Directory サーバー（ドメインコントローラ）	Windows ドメインクライアント
サービス	Active Directory	—
SMARTACCESS	SMARTACCESS/Premium	

重要

- 「Active Directory管理」は、連携したActive Directoryが管理するドメインが管理対象になります。
- 「Active Directory 連携クライアント」のコンピュータは、ドメインに参加している必要があります。
- Active Directory のユーザーや組織単位（OU）は、Active Directory での登録が必要です。Active Directory については、Windows Server のヘルプをご覧ください。

Active Directory 連携の導入ステップ

Active Directory 連携を導入するには、Active Directory サーバーに「Active Directory 管理」、クライアントコンピュータに「Active Directory 連携クライアント」を導入します。
主な導入手順は次のとおりです。

1 SMARTACCESS/Premium のインストール（→ P.58）

2 「Active Directory 管理」のインストール（→ P.130）

3 Active Directory 連携クライアントの構成

詳しくは、『リファレンスガイド』の「機能編」－「Active Directory 連携」をご覧ください。

1. Active Directory との連携
   Active Directory との連携、および Active Directory に接続して設定情報の適用が必要かどうかを確認する間隔を設定します。
2. ユーザー情報の取得先の指定
   ユーザー情報の取得先の Active Directory を設定します。

4 環境設定によるセキュリティ環境の構築

詳しくは、『リファレンスガイド』の「機能編」－「Active Directory 連携」をご覧ください。

Active Directory 管理のインストール

「Active Directory 管理」のインストールは、インストーラを実行して画面の指示に従いながら行います。

重要

- 「Active Directory 管理」のインストールをするには、ドメイン管理者権限で Windows にログオンしている必要があります。
- 「Active Directory 管理」をインストールする前に、使用中のアプリケーションはすべて終了させてください。
- ハードディスクに十分な空き容量があることをご確認ください。

1 「SMARTACCESS/Premium」CD-ROM をセットします。

2 「スタート」ボタン→「ファイル名を指定して実行」の順にクリックします。

3 「名前」に次のように入力し、「OK」をクリックします。

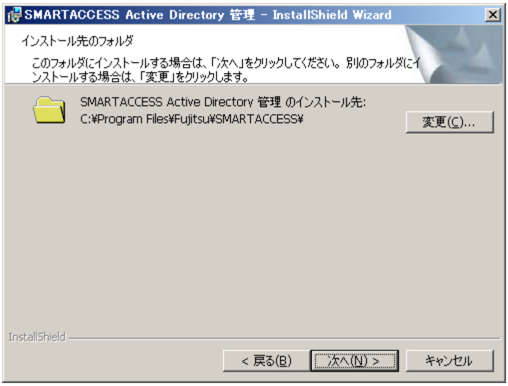
[CD/DVD ドライブ]:¥SAPremium¥Active Directory¥Setup¥setup.exe

「SMARTACCESS Active Directory 管理の InstallShield ウィザードへようこそ」と表示されます。



4 「次へ」をクリックします。

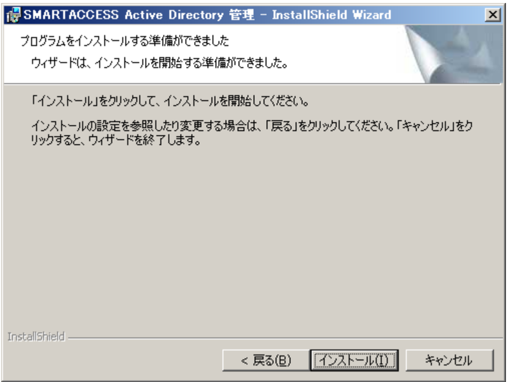
「インストール先のフォルダ」と表示されます。



5 インストール先を確認し、「次へ」をクリックします。

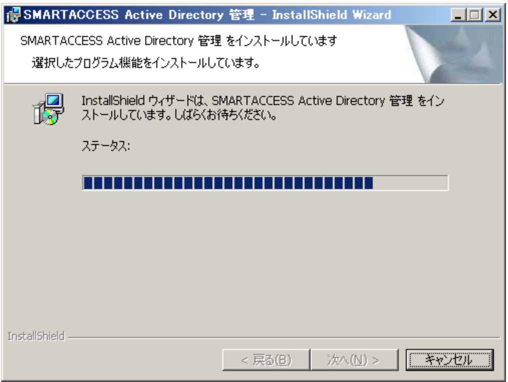
インストール先を変更する場合は、「変更」をクリックして別のインストール先フォルダを指定します。

「プログラムがインストールできる準備ができました」と表示されます。

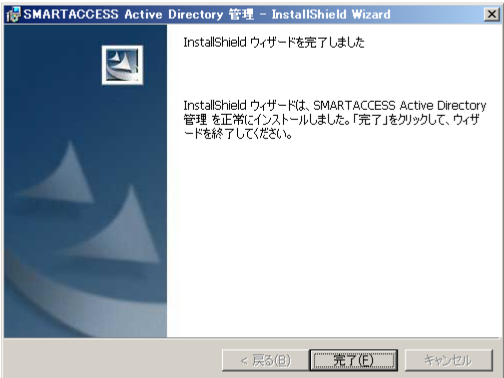


6 「インストール」をクリックして、インストールを開始します。

「SMARTACCESS Active Directory 管理をインストールしています」と表示されます。

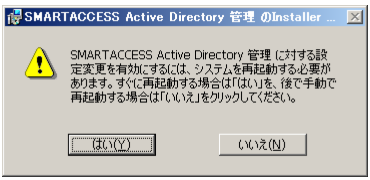


インストールが正常に完了すると、「Install Shield ウィザードを完了しました」と表示されます。



7 「完了」をクリックします。

再起動を要求するメッセージが表示されます。



8 「はい」をクリックして、Windows を再起動します。

「Active Directory 管理」のインストール情報を有効にするには、Windows の再起動が必要です。

重要

- Active Directory 管理から環境設定を行う場合、あらかじめ SMARTACCESS/Premium がインストールされている環境で初期値の情報を準備する必要があります。
  操作手順は次の通りです。
  1. SMARTACCESS/Premium がインストールされている環境で、「バックアップツール」を使用してバックアップを行い「環境設定ファイル（F5FZCFGM.fcb）」を作成します。詳しくは、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧ください。
  2. 「バックアップツール」で作成した「環境設定ファイル」を「Active Directory 管理」がインストールされたフォルダに格納します。
     格納先は次の通りです。
     C:¥Program Files¥Fujitsu¥SMARTACCESS¥Data
     なお、インストール時にインストールフォルダを変更した場合は、変更先のインストールフォルダにある「¥Data」に格納してください。
  3. 「Active Directory 管理」から環境設定を行います。

2 バイオ認証装置連携

バイオ認証装置連携は、「バイオ認証装置 Secure Login Box」で管理する指紋、および静脈による認証（バイオ認証）を SMARTACCESS で実現する機能です。認証デバイスから入力された指紋、または静脈と、バイオ認証装置が管理する認証用の指紋や静脈を照合して本人認証を行います。
バイオ認証装置との連携によりユーザーの認証用の指紋や静脈を一括管理することができます。

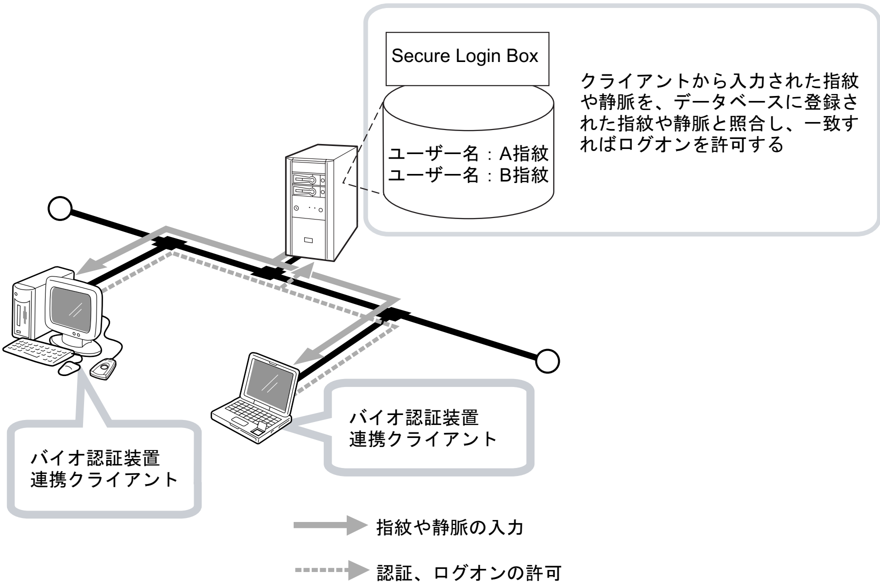
バイオ認証装置連携をお使いになるために必要なものは、次のとおりです。

□ バイオ認証装置

認証用の指紋、および静脈情報を一括管理します。

□ バイオ認証装置連携クライアント

バイオ認証装置のクライアントになるコンピュータは、SMARTACCESS でバイオ認証装置と連携することで、指紋や静脈による Windows ログオンやアプリケーションログオンが利用できます。バイオ認証装置によって指紋や静脈認証されます。



バイオ認証装置連携の導入

バイオ認証装置連携を導入するには、ネットワーク上にサーバーとしてバイオ認証装置を導入し、「バイオ認証装置連携クライアント」には SMARTACCESS/Premium を導入します。主な導入手順は次のとおりです。

1 SMARTACCESS/Premium のインストール（→ P.58）

2 バイオ認証装置のセットアップとユーザー登録

詳しくは、バイオ認証装置のマニュアルをご覧ください。

3 バイオ認証装置連携クライアントの構成

詳しくは、『リファレンスガイド』の「機能編」－「バイオ認証装置連携」をご覧ください。

1. バイオ認証装置を使用するよう設定
2. アカウントの登録
3. Windows ログオン（→ P.85）やアプリケーションログオン（→ P.86）の設定

必要に応じて設定します。

4. 認証用のユーザー情報の登録

   認証用の指紋や静脈データを、バイオ認証装置に登録します。

Memo

7

第 7 章

困ったときには

おかしいなと思ったときや、わからないことがあったときの
対処方法について説明しています。

1 セキュリティチップ

□ BIOS でセキュリティチップの設定を変更できない

BIOS で、セキュリティチップの使用や、セキュリティチップのデータをクリアする設定を行うためには、管理者用パスワードの設定が必要です。管理者用パスワードが設定されているか確認してください。

□ Infineon TPM Professional Package（Infineon Security Platform）ユーティリティがインストールできない

ソフトウェアをインストールするには、BIOS でセキュリティチップを使用する設定になっている必要があります。BIOS の設定を確認してください。
BIOS の設定については、コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧ください。

□ Windows ログオン時に機器が変更された旨のエラーメッセージが表示される

前回の起動からハードウェアの構成や設定が変更された可能性があります。ハードウェア構成や BIOS 設定など変更されていないか確認してください。変更があった場合は、機器を登録したときの状態に戻してください。
なお、変更の内容によっては、機器を登録したときの状態に戻しても、エラーメッセージが解除されない場合があります。詳しくは『リファレンスガイド』の「機能編」－「Windows ログオン」－「機器監査」をご覧ください。

□ Windows ログオン時にユーザーキーパスワードエラーになる

SMARTACCESS による Windows ログオンを有効にしている場合には、Windows のパスワードではなくセキュリティチップのユーザーキーパスワードを入力してください。

□ EFS が利用できない

EFS を利用するにはハードディスクが NTFS でフォーマットされていることが必要です。FAT32 のドライブでは EFS を利用することはできません。なお、Windows XP Home Edition では、EFS は利用できません。

□ BIOSセットアップでセキュリティチップを使用しない設定にしたら、Windows にログオンできなくなった

「SMARTACCESS による Windows ログオン」を「する」に設定した状態で、次のように BIOS セットアップのセキュリティチップを使用しない設定にすると、セキュリティチップに保存していた Windows パスワードが利用できず、Windows にログオンできなくなることがあります。

・「Disabled」（FMV-ESPRIMO、FMV ロングライフパソコン、CELSIUS シリーズの場合）
・「使用しない」（FMV-LIFEBOOK、FMV-STYLISTIC の場合）

その場合は次のように設定し直すか、「回避パスワード」でログオンする必要があります。

・「Enabled」（FMV ロングライフパソコン、CELSIUS シリーズの場合）
・「使用する」（FMV-LIFEBOOK、FMVSTYLISTIC の場合）

BIOS の設定については、コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧ください。
なお、「回避パスワード」でログオンしても、セキュリティチップで保護された環境は安全に管理されています。

回避パスワードについては、『リファレンスガイド』の「機能編」－「Windows ログオン」－「認証回避」をご覧ください。

□ ハードウェア構成を変更したために Windows にログオンできなくなった

ハードウェアの構成を変更すると、SMARTACCESS の機器監査機能により Windows にログオンできなくなります。その場合はハードウェア構成を登録したときの設定に戻すか、機器構成を登録しなおす必要があります。設定方法については、『リファレンスガイド』の「機能編」－「Windows ログオン」－「機器監査」をご覧ください。

□ リストアを行うとユーザーキーパスワードが変わることがある

リストアを行うと、ユーザーキーパスワードにはバックアップを行った時点でのパスワードが設定されます。
そのため、バックアップ後にユーザーキーパスワードを変更しても、復元すると、バックアップを行った時点でのパスワードに戻ります。

□ ソフトウェアのインストール時に「アプリケーションエラー」が表示されることがある

「インストールと設定」（→ P.51）の手順に従わずにソフトウェアをインストールすると、「アプリケーションエラー」が表示されることがあります。
もし表示された場合、ソフトウェアのインストールを引き続き行い、インストール終了後は表示画面に従って Windows を再起動してください。再起動後は正常に動作します。

□ SMARTACCESS でユーザ初期化を行うと、失敗することがある

SMARTACCESS をインストール時に、セキュリティチップがクリアされていない状態で行うと、ユーザ初期化に失敗することがあります。インストール時にはセキュリティチップがクリアされていたかどうか確認してください。クリアされていなかった場合には SMARTACCESS をアンインストールし、BIOS でセキュリティチップをクリアした後、再度 SMARTACCESS をインストールしてください。

2 指紋センサー

□ 指紋登録時にエラー表示される

- 指の置き方が正しいか確認してください。指が正しく置かれていない、または、指を置く方向が毎回ずれていると登録できないことがあります（→「認証デバイスについて」－「指紋センサー」－「取り扱い方」（→ P.24）。
- 指が乾燥していませんか。
  手を洗う、指に息を吹きかけるなど指がしっとりする程度の湿り気を与えることで改善されることがあります（→「認証デバイスについて」－「指紋センサー」－「取り扱い方」－「取り扱い上の注意事項」（→ P.26）。
- 指が濡れていませんか。
  乾いたハンカチなどで指の湿り気を拭き取ることで改善されることがあります（→「認証デバイスについて」－「指紋センサー」－「取り扱い方」－「取り扱い上の注意事項」（→ P.26）。
- センサー表面を確認してください。汚れていたり、汗などの水分が付着していると指紋が読み取れない場合があります（→「認証デバイスについて」－「指紋センサー」－「取り扱い方」－「取り扱い上の注意事項」（→ P.26）。
- 異なる指で再度登録してください。

□ 指紋照合時にエラー表示される

- 指の置き方が正しいか確認してください。指が正しく置かれていないと照合できないことがあります（→「認証デバイスについて」－「指紋センサー」－「取り扱い方」（→ P.24）。
- 指が乾燥していませんか。
  手を洗う、指に息を吹きかけるなど指がしっとりする程度の湿り気を与えることで改善されることがあります（→「認証デバイスについて」－「指紋センサー」－「取り扱い方」－「取り扱い上の注意事項」（→ P.26）。
- 指が濡れていませんか。
  乾いたハンカチなどで指の湿り気を拭き取ることで改善されることがあります（→「認証デバイスについて」－「指紋センサー」－「取り扱い方」－「取り扱い上の注意事項」（→ P.26）。
- センサー表面を確認してください。汚れていたり、汗などの水分が付着していると指紋が読み取れない場合があります（→「認証デバイスについて」－「指紋センサー」－「取り扱い方」－「取り扱い上の注意事項」（→ P.26）。
- 登録したもう片方の指で照合してください。

3 静脈センサー

静脈センサーをお使いのときのトラブルの対処方法については、静脈センサーに添付のマニュアルをご覧ください。

4 FeliCa 対応リーダ／ライタ

□ FeliCa 対応非接触 IC カードを使って Windows ログオンを行っている場合、BIOS セットアップの「FeliCa デバイス」の設定を「使用しない」にすると、Windows にログオンできなくなる

FeliCa 対応非接触 IC カードを使って Windows ログオンを行っている場合は、BIOS セットアップの「FeliCa デバイス」の設定を「使用する」にしてください。BIOS セットアップの設定については、コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧ください。

□ SMARTACCESS/Premium を利用している場合、FeliCa リーダー / ライターソフトウェアをアンインストールすると、Windows が起動できなくなる

FeliCaリーダー /ライターソフトウェアをアンインストールする場合は、SMARTACCESS/Premiumをアンインストールした後で行ってください。
FeliCaリーダー /ライターソフトウェアがインストールされていない状態でSMARTACCESS/PremiumによるログオンをWindowsが正常に起動できなくなります。Windowsが正常に起動できなくなった場合は、「富士通ハードウェア修理相談センター」、またはご購入元にお問い合わせください。

5 スマートカードリーダ／ライタ、スマートカードホルダー

スマートカードリーダ／ライタ、およびスマートカードホルダーをお使いのときに表示されるエラーメッセージについては、コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧ください。

6 その他のトラブルシューティング

SMARTACCESS インストール、アンインストール時のエラーメッセージ

・アプリケーション「Secure Login Light」をアンインストールしてからドライバをアンインストールしてください。
SMARTACCESS がインストールされている状態で、指紋ドライバをアンインストールしようとしました。「Secure Login Light」は SMARTACCESS が動作するために必要なコンポーネントの 1 つです。
SMARTACCESS をアンインストールしてから、指紋ドライバをアンインストールしてください。

SMARTACCESS Active Directory 管理インストール時のエラーメッセージ

・アトリビュートの作成に失敗しました。（スキーマ名、詳細エラーコード）
次のような場合に、Active Directory 管理で使用するスキーマの拡張に失敗したときに表示されます。
- サーバー上で Active Directory 機能の設定が行われていない
- Domain Admin 権限のないユーザーでインストールを行った
- サーバーをネットワークに正しく接続しない状態でインストールを行った
再度「Active Directory 管理」のインストールを行ってください。

その他

この章に記載されていないトラブルやエラーメッセージの対処方法については、『リファレンスガイド』の「付録」－「トラブルシューティング」をご覧ください。

8

第 8 章

付録

1 用語集

用語	説明
Active Directory	Windows Server のディレクトリ サービスで、Windows Server の分散ネットワークの基盤となるものです。
FENCE-G	コンピュータの各種ポートの読み書きを制御できるソフトウェアです。
PIN（Personal Identification Number）	IC カード（FeliCa 方式）やスマートカードを使うときのパスワードの一種です。
Portshutter	コンピュータの各種ポートを使用制限できるソフトウェアです。FMV シリーズや CELSIUS シリーズのコンピュータに添付されています。
Security Platform（Infineon TPM Professional Package）	セキュリティチップを使用するために必要なユーティリティです。
SMARTACCESS アカウント	SMARTACCESS を利用するためのアカウント情報です。ユーザー名とパスワードを登録します。
Systemwalker	セキュリティ管理、ジョブ管理などを行う統合運用管理ソフトウェアです。本製品と連携することで、利用イベントの集中管理やファイル暗号化ができます。
Windows ログオン情報	認証デバイスに登録する、Windows にログオンするときのユーザー名、パスワード、ドメイン名などです。
アプリケーションログオン情報	認証デバイスに登録するソフトウェアや Web サイトにログオンするときのユーザー名、パスワードなどです。
暗号鍵	情報を暗号化または復号するときに使用する、特定のデータです。
オブジェクト	Active Directory の用語で、ユーザーやコンピュータ、組織単位（OU）を指します。
カード IDm	IC カード（FeliCa 方式）のシリアル番号です。カード製造時に一意に割り当てられます（カードに刻印された番号とは異なります）。
カード抜き取り	IC カード（FeliCa 方式）やスマートカードをセットした状態から外す操作です。
管理者	本製品を管理する人（セキュリティポリシーを設定したり、管理したりする人）です。 通常、Windows アカウントは管理者（Administrators）権限です。
管理者 PIN	管理機能を利用する場合に必要となる PIN です。
管理者権限カード	カード管理リストで、管理者属性が設定されているカードです。
機器監査	あらかじめ機器構成を登録し、Windows 起動時の機器構成と比較することで、機器構成が変更されていないかを監査する機能です。
機器構成	BIOS 設定のハードウェア構成やメモリスロットの構成など、使用しているコンピュータのハードウェア構成です。

用語	説明
証明書	本人を証明する電子証明書のことです。本製品では、Windows ログオンや Web サーバーへのアクセスにお使いになれます。
所有者	IC カード（FeliCa 方式）やスマートカードなど、持ち運び可能な認証デバイスを所有する人です。
所有者 PIN	通常使用する PIN です。
シングルサインオン機能	ソフトウェアや Web サイトなどにログオンするとき、一度ログオン認証に成功すれば、以降は同一ユーザーがコンピュータを継続使用しているものとしてログオン認証を省略できるようになる機能です。
セキュリティチップ	TPM（Trusted Platform Module）と呼ばれるセキュリティ用の専用ハードウェアチップです。 セキュリティチップは内部に暗号鍵を保持し、ソフトウェアで使用するパスワードなどを暗号化します。セキュリティチップに保持された暗号鍵は外部に出す方法がありませんので安全に管理できます。
セット	IC カード（FeliCa 方式）を FeliCa 対応リーダ／ライタに載せておくことです。
組織単位（OU）	Active Directory のユーザーやコンピュータをまとめるための入れもののことです。ユーザーやコンピュータを組織化する場合などに利用します。
タッチ	IC カード（FeliCa 方式）を FeliCa 対応リーダ／ライタに一時的に接触させる操作です。
認証デバイス	認証を行う手段や装置です。 本製品では、セキュリティチップ、指紋センサー、静脈センサー、FeliCa 対応リーダ／ライタ、スマートカードリーダ／ライタ、およびスマートカードホルダーを指します。
バイオ認証装置	指紋や静脈を利用して認証する認証サーバーです。
バイオパスワード	指紋や静脈を登録するときや、指紋や静脈でのログオンを回避するときに使用するパスワードです。
パスワード入力画面情報／パスワード入力画面情報ファイル	アプリケーションログオン機能を使ってログオンするソフトウェアや Web サイトのパスワード入力画面の情報を格納しているファイルです。
フィールド ID	ソフトウェアのパスワードやユーザー名を入力する各入力フィールド、およびボタンに割り振られている ID です。
ポーリング	スマートカードをリーダ／ライタから抜き取ったり、IC カード（FeliCa 方式）をリーダ／ライタにタッチしたりしたときに、コンピュータのロックや強制ログオフなどを行い、コンピュータを不正な使用から保護することです。
ユーザーキーパスワード	セキュリティチップを使用する際に入力するパスワードです。セキュリティチップを使用するユーザー毎に設定します。基本ユーザーパスワードと表現されることもあります。
ユーザー情報	Windows ログオン情報およびアプリケーションログオン情報などの認証用の情報のことです。例えば、ユーザー名やパスワード、指紋、静脈、PIN などを指します。
利用者	本製品を管理者のもとで使う人です。

用語	説明
連携ソフトウェア	SMARTACCESS の機能を拡張させるために、連携できる他製品のこのマニュアルでの総称です。Portshutter、FENCE-G、FENCE-Pro、および Systemwalker シリーズです。

SMARTACCESS ファーストステップガイド
（認証デバイスをお使いになる方へ）

B5FJ-1001-01 Z2-01

発 行 日　2006 年 10 月
発行責任　富士通株式会社